Intro

RoadMap

TODO

Download everything in a single PDF

To download everything here in a single pdf, click here

Basics

Well Ordering Principle And Division Algorithm

Well Ordering Principle: Every nonempty set of positive integers contains a smallest member. (*Take is as an axiom*)

Theorem 1.1 (Division Algorithm): Let a and b be integers with $b > 0$. Then there exist unique integers q and r with the property that $a = bq + r$, where $0 \leq r < b$.

Proof: We begin with the existence portion of the theorem. Consider the set $S = \{a - bk \mid k \text{ is an integer and } a - bk \geq 0\}$. If $0 \in S$, then b divides a and we may obtain the desired result with $q = a/b$ and $r = 0$. Now assume $0 \notin S$. Since S is nonempty [if $a > 0, a - b.0 \in S$; if $a < 0, a - b(2a) = a(1 - 2b) \in S$; $a \neq 0$ since $0 \notin S$], we may apply the Well Ordering Principle to conclude that S has a smallest member, say $r = a - bq$. Then $a = bq + r$ and $r \geq 0$, so all that remains to be proved is that $r < b$. If $r \geq b$, then $a - b(q + 1) = a - bq - b = r - b \geq 0$, so that $a - b(q + 1) \in S$. But $a - b(q + 1) < a - bq$, and $a - bq$ is the smallest member of S. So, $r < b$. To establish the uniqueness of q and r, let us suppose that there are integers q, q', r, and r' such that $a = bq + r, 0 \leq r < b$, and $a = bq' + r', 0 \leq r' < b$. For convenience, we may also suppose that $r' \geq r$. Then $bq + r = bq' + r'$ and $b(q - q') = r' - r$. So, b divides $r' - r$ and $0 \leq r' - r \leq r' < b$. It follows that $r' - r = 0$, and therefore $r' = r$ and $q' = q$. ■

GCD

The greatest common divisor of two nonzero integers a and b is the largest of all common divisors of a and b. We denote this integer by $gcd(a, b)$. When $gcd(a, b) = 1$, we say a and b are relatively prime.

Theorem 1.2 (GCD is a linear combination): For any nonzero integers a and b, there exist integers s and t such that $gcd(a, b) = as + bt$. Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Proof: Consider the set $S = \{am + bn \mid m, n \text{ are integers and } am + bn > 0\}$. Since S is obviously nonempty (if some choice of m and n makes $am + bn < 0$, then replace m and n by $-m$ and $-n$), the Well Ordering Principle asserts that S has a smallest member, say, $d = as + bt$. We claim that $d = gcd(a, b)$. To verify this claim, use the division algorithm to write $a = dq+r$, where $0 \leq r < d$. If $r > 0$, then $r = a-dq = a-(as+bt)q = a-asq-btq = a(1-sq)+b(-tq) \in S$, contradicting the fact that d is the smallest member of S *(Note that we wanted to show $a - dq < d$ which is obviously true as $r < d$.)*. So, $r = 0$ and d divides a. Analogously (or, better yet, by symmetry), d divides b as well. This proves that d is a common divisor of a and b. Now suppose d' is another common divisor of a and b and write $a = d'h$ and $b = d'k$. Then $d = as+bt = (d'h)s+(d'k)t = d'(hs + kt)$, so that d' is a divisor of d. Thus, among all common divisors of a and b, d is the greatest.

Corollary: If a and b are relatively prime, then there exist integers s and t such that $as + bt = 1$.

Theorem 1.3 (Euclid's Lemma): If p is a prime that divides ab, then p divides a or p divides b. (easy to see)

Fundamental theorem of arithmetic (*to be proved later*): Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear.

LCM

The least common multiple of two nonzero integers a and b is the smallest positive integer that is a multiple of both a and b.

Modulo Arithmetic

When $a = qn + r$, where q is the quotient and r is the remainder upon dividing a by n, we write $a \bmod n = r$.

In general, if a and b are integers and n is a positive integer, then $a \bmod n = b \bmod n$ if and only if n divides $a - b$. (easy to see)

Examples:

- $-2 \bmod 15 = 13$ since $-2 = (-1)15 + 13$.
- Consider the statement, "The sum of the cubes of any three consecutive integers is divisible by 9." This statement is equivalent to checking that the equation $(n^3 + (n+1)^3 + (n+2)^3) \bmod 9 = 0$ is true for all integers n. Because of properties of modular arithmetic, to prove this, all we need do is check the validity of the equation for $n = 0, 1, \ldots, 8$.
- We use mod 3 arithmetic to show that there are no integers a and b such that $a^2 - 6b = 2$. To see this, suppose that there are such integers. Then, taking both sides modulo 3, there is an integer solution to $a^2 \bmod 3 = 2$. But trying $a = 0, 1$, and 2 we obtain a contradiction.

Mathematical Induction

First principle of mathematical induction

Let S be a set of integers containing a. Suppose S has the property that whenever some integer $n \geq a$ belongs to S, then the integer $n + 1$ also belongs to S. Then, S contains every integer greater than or equal to a.

Second principle of mathematical induction

Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S. Then, S contains every integer greater than or equal to a.

Examples:

- We will use the Second Principle of Mathematical Induction with $a = 2$ to prove the existence portion of the Fundamental Theorem of Arithmetic. Let S be the set of integers greater than 1 that are primes or products of primes. Clearly, $2 \in S$. Now we assume that for some integer n, S contains all integers k with $2 \leq k < n$. We must show that $n \in S$. If n is a prime, then $n \in S$ by definition. If n is not a prime, then n can be written in the form ab, where $1 < a < n$ and $1 < b < n$. Since we are assuming that both a and b belong to S, we know that each of them is a

prime or a product of primes. Thus, n is also a product of primes. This completes the proof. ■

- The Quakertown Poker Club plays with blue chips worth \$5.00 and red chips worth \$8.00. What is the largest bet that cannot be made?

  To gain insight into this problem, we try various combinations of blue and red chips and obtain 5, 8, 10, 13, 15, 16, 18, 20, 21, 23, 24, 25, 26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40. It appears that the answer is 27. But how can we be sure? Well, we need only prove that every integer greater than 27 can be written in the form $a*5+b*8$, where a and b are nonnegative integers. This will solve the problem, since a represents the number of blue chips and b the number of red chips needed to make a bet of $a*5+b*8$. For the purpose of contrast, we will give two proofs—one using the First Principle of Mathematical Induction and one using the Second Principle. Let S be the set of all integers greater than or equal to 28 of the form $a*5+b*8$, where a and b are nonnegative. Obviously, $28 \in S$. Now assume that some integer $n \in S$, say, $n = a*5+b*8$. We must show that $n+1 \in S$. First, note that since $n \geq 28$, we cannot have both a and b less than 3. If $a \geq 3$, then $n+1 = (a*5+b*8)+(-3*5+2*8) = (a-3)*5+(b+2)*8$. If $b \geq 3$, then $n+1 = (a*5+b*8)+(5*5-3*8) = (a+5)*5+(b-3)*8$. This completes the proof. To prove the same statement by the Second Principle, we note that each of the integers 28, 29, 30, 31, and 32 is in S. Now assume that for some integer $n > 32$, S contains all integers k with $28 \leq k < n$. We must show that $n \in S$. Since $n-5 \in S$, there are nonnegative integers a and b such that $n-5 = a*5+b*8$. But then $n = (a+1)*5+b*8$. Thus n is in S.

Equivalence Relation

Note: If A is any non empty set, then a subset R of $A \times A$ is defined as a relation on A.

An equivalence relation on a set S is a set R of ordered pairs of elements of S such that

1. $(a, a) \in R$ for all $a \in S$ (reflexive property).
2. $(a, b) \in R$ implies $(b, a) \in R$ (symmetric property).
3. $(a, b) \in R$ and $(b, c) \in R$ imply $(a, c) \in R$ (transitive property).

When R is an equivalence relation on a set S, it is customary to write aRb instead of $(a, b) \in R$

If $\sim$ is an equivalence relation on a set S and $a \in S$, then the set $[a] = \{x \in S \mid x \sim a\}$ is called the equivalence class of S containing a.

Examples:

- Let S be the set of integers and let n be a positive integer. If $a, b \in S$, define $a \equiv b$ if $a \bmod n = b \bmod n$ (that is, if $a - b$ is divisible by n). Then $\equiv$ is an equivalence relation on S and $[a] = \{a + kn \mid k \in S\}$.

Partition

A partition of a set S is a collection of nonempty disjoint subsets of S whose union is S.

Theorem 1.4: The equivalence classes of an equivalence relation on a set S constitute a partition of S . Conversely, for any partition P of S , there is an equivalence relation on S whose equivalence classes are the elements of P . (First part is easy, for second part, Define $a \sim b$ if a and b belong to the same subset in the collection.)

Functions

Definition: A function (or mapping) ϕ from a set A to a set B is a rule that assigns to each element a of A exactly one element b of B.

Definition: Let $\phi : A \to B$ and $\psi : B \to C$. The composition $\psi\phi$ is the mapping from A to C defined by $(\psi\phi)(a) = \psi(\phi(a))$ for all a in A .

Definition: A function f from a set A is called one-to-one if for every $a_1, a_2 \in A, f(a_1) = f(a_2)$ implies $a_1 = a_2$.

Alternatively f is one-to-one if $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$

Definition: In symbols, $\phi : A \to B$ is onto if for each b in B there is at least one a in A such that $\phi(a) = b$.

Properties

Given functions $\alpha : A \to B, \beta : B \to C$, and $\gamma : C \to D$, then

1. $\gamma(\beta\alpha) = (\gamma\beta)\alpha$ (associativity).
2. If α and β are one-to-one, then $\beta\alpha$ is one-to-one.
3. If α and β are onto, then $\beta\alpha$ is onto.
4. If α is one-to-one and onto, then there is a function α^{-1} from B onto A such that $\left(\alpha^{-1}\alpha\right)(a) = a$ for all a in A and $\left(\alpha\alpha^{-1}\right)(b) = b$ for all b in B .

Proof:

1. Let $a \in A$. Then $(\gamma(\beta\alpha))(a) = \gamma((\beta\alpha)(a)) = \gamma(\beta(\alpha(a)))$. On the other hand, $((\gamma\beta)\alpha)(a) = (\gamma\beta)(\alpha(a)) = \gamma(\beta(\alpha(a)))$. So , $\gamma(\beta\alpha) = (\gamma\beta)\alpha$
2. Easy

3. Easy
4. Easy

Groups

Definition

Let G be a set together with a binary operation (usually called multiplication that assigns to each ordered pair (a, b) of elements of G an element in G (known as closure condition) denoted by ab. We say G is a group under this operation if the following three properties are satisfied.

1. Associativity. The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G.
2. Identity. There is an element e (called the identity) in G such that $ae = ea = a$ for all a in G.
3. Inverses. For each element a in G, there is an element b in G (called an inverse of a) such that $ab = ba = e$.

Be sure to verify closure when testing for a group.

Notice that if b is the inverse of a, then a is the inverse of b.

If a group has the property that $ab = ba$ for every pair of elements a and b, we say the group is Abelian. A group is non-Abelian if there is some pair of elements a and b for which $ab \neq ba$.

Examples:

- In a group if each element is equal to its inverse then it is abelian. (easy to show)
- Any group of order 5 or less is abelian.

  Proof: Any group of order 4 can only be written in a way $G = \{e, a, b, ab\}$ as any other way will fail one or more group axioms. Clearly this is abelian.

  For order 5, let $G = \{e, a, b, c, d\}$. Now we need to assign a element for each of $2 \times \binom{4}{2} = 12$ combinations, but since we are only interested in abelian property, we need to consider only 6 combinations.

  Let, $ab = e \rightarrow (ab)c = c = a(bc) \rightarrow bc = a^{-1}c$

thus $bc \neq b, c, a^{-1} = b$ nor can it be e as then $bc = ab \rightarrow (ab)c = c = a(bc) = a$. Thus choices available are a, d.

Also in general if $k_1 k_2 = e \rightarrow k_2 k_1 = e$

If $bc = a \rightarrow \because a^{-1} = b \rightarrow a = a^2 b = cb$

Similarly $acb = a(cb) = a^2 \rightarrow ac = a^2 b^{-1} = ca$

Similarly choices for bd are c, a but if $bc = a \rightarrow bd \neq a$ as then $bc = bd \rightarrow c = d$ and thus $bd = c$

Now using associativity of cbd we get $d = ac = ca$ (can be worked out) thus $db = cab = c = bd$ and $da = caa = c^2$, $ad = aac = c^2$

$dc = ac^2 = a^5$, $cd = cca = c^2 a = a^5$ hence if it forms the group, it is abelian.

Similarly one can try for other cases as they are symmetric because if we would have started with $bc = a$ which is equivalent to starting with $ab = c, d, etc..$ we would arrive at $ab = e$ or d...

- The set of integers under ordinary multiplication is not a group. Since property 3 fails (number 1 is the identity).
- The set $A(S)$ of all one to one mappings of a non empty set S onto itself is a group wrt the product of mappings (i.e. function compositions).
- The set S of positive irrational numbers together with 1 under multiplication satisfies the three properties given in the definition of a group but is not a group. Indeed, $\sqrt{2} * \sqrt{2} = 2$, so S is not closed under multiplication.
- The set $Z_n = \{0, 1, ..., n-1\}$ for $n \geq 1$ is a group under addition modulo n. For any $j > 0$ in Z_n, the inverse of j is $n - j$. This group is usually referred to as the group of integers modulo n.
- Note: An integer a has a multiplicative inverse modulo n if and only if a and n are relatively prime (easy to prove) . So, for each $n > 1$, we define $U(n)$ to be the set of all positive integers less than n and relatively prime to n. Then $U(n)$ is a group under multiplication modulo n (very important observation is that if b is the multiplicative inverse of a then $ab \bmod n = 1$, define $b \bmod n = k \rightarrow ak \bmod n = 1$ thus $k \in U(n)$). (Note that this set is closed under this operation (Proof: $at_1 + nt_2 = 1, bt_3 + nt_4 = 1 \Rightarrow abt_1 t_3 + at_1 nt_4 + nt_2 bt_3 + n^2 t_2 t_4 \Rightarrow ab(..) + n(..) = 1$).) For $n = 10$, we have $U(10) = \{1, 3, 7, 9\}$.
- The set of integers under subtraction is not a group, since the operation is not associative.
- The set $\{1, 2, ..., n-1\}$ is a group under multiplication modulo n if and only if n is prime (as each element must possess an inverse).

- The set of all 2×2 matrices with determinant 1 with entries from Q (rationals), $\mathbf{R}$(reals), $\mathbf{C}$(complex numbers), or Z_p(p a prime) is a non-Abelian group under matrix multiplication. This group is called the special linear group of 2×2 matrices over $Q, \mathbf{R}$, or Z_p, respectively. If the entries are from F, where F is any of the above, we denote this group by $SL(2, F)$. For the group $SL(2, F)$, the formula for the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ simplifies to $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. When the matrix entries are from Z_p, we use modulo p arithmetic to compute determinants, matrix products, and inverses. To illustrate the case $SL\left(2, Z_5\right)$ consider the element $A = \begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}$. Then $\det\ A = (3 \cdot 4 - 4 \cdot 4) \bmod 5 = -4 \bmod 5 = 1$, and the inverse of A is $\begin{bmatrix} 4 & -4 \\ -4 & 3 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}$. Note that $\begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix} \begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ when the arithmetic is done modulo 5
- Let F be any of $Q, \mathbf{R}, \mathbf{C}$, or Z_p(p a prime). The set $GL(2, F)$ of all 2×2 matrices with nonzero determinants and entries from F is a non-Abelian group under matrix multiplication. When F is Z_p, modulo p arithmetic is used to calculate determinants, matrix products, and inverses. The usual formula for the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ remains valid for elements from $GL\left(2, Z_p\right)$, provided we interpret division by $ad - bc$ as multiplication by the inverse of $(ad - bc)$ modulo p. For example, in $GL\left(2, Z_7\right)$ consider $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}$. Then the determinant $(ad - bc) \bmod 7$ is $(12 - 30)\ \text{mod}7 = -18 \bmod 7 = 3$ and the inverse of 3 is 5[since$(3 \cdot 5))\ \bmod 7 = 1$]. So, the inverse of $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix}$ is $\begin{bmatrix} 3 \cdot 5 & 2 \cdot 5 \\ 1 \cdot 5 & 4 \cdot 5 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix}$ [The reader should check that $\begin{bmatrix} 4 & 5 \\ 6 & 3 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in $GL\left(2, Z_7\right)$] The group $GL(n, F)$ is called the general linear group of $n \times n$ matrices over F.
- The set of all symmetries of the infinite ornamental pattern in which arrowheads are spaced uniformly a unit apart along a line is an Abelian group under composition. Let T denote a translation to the right by one unit, T^{-1} a translation to the left by one unit, and H a reflection across the horizontal line of the figure. Then, every member of the group is of the form $x_1 x_2 \cdots x_n$, where each $x_i \in \left\{T, T^{-1}, H\right\}$. In this case, we say that T, T^{-1}, and H generate the group.

Figure 1: image

Properties

The following three theorems were very easy to prove for me.

Theorem 2.2: In a group G, the right and left cancellation laws hold; that is , $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$ (easy to see)

A consequence of the cancellation property is the fact that in a Cayley table for a group, each group element occurs exactly once in each row and column. **Proof:** Each element occurs at least once as suppose M doesn't occur in column of R, its not possible as we have $R^{-1}M =$ something (binary composition). Now to prove at most 1, we have $RM = K$ and $RN = K \Rightarrow RM = RN \Rightarrow M = N$.

Theorem 2.3: Inverse is unique (easy to prove)

So we will unambiguously denote the inverse by g^{-1}

Similarly, when n is a positive integer, the associative law allows us to use g^n to denote the unambiguous product We define $g^0 = e$. When n is negative, we define $g^n = \left(g^{-1}\right)^{|n|}$ [for example, $g^{-3} = \left(g^{-1}\right)^3$.] familiar laws of exponents hold for groups; that is, for all integers m and n and any group element g, we have $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$

Note: $ax = b \Rightarrow x = a^{-1}b$ *which is unique as inverse is unique*

Also, one must be careful with this notation when dealing with a specific group whose binary operation is addition and is denoted by "+"

Multiplicative Group	Additive Group				
		$a \cdot b$ or ab	Multiplication	$a + b$	Ad
		e or 1	Identity or one	0	Zer
		a^{-1}	Multiplicative inverse of a	$-a$	Ad
		a^n	Power of a	na	Mu
		ab^{-1}	Quotient	$a - b$	Dif

So, g^{-3} means $(-g) + (-g) + (-g)$ and is written as $-3g$.

As is the case for real numbers, we use $a - b$ as an abbreviation for $a + (-b)$.

Note: $a^2\left(bcdb^2\right) = a^2b(cd)b^2 = \left(a^2b\right)(cd)b^2 = a(abcdb)b$

Theorem 2.4: For group elements a and $b, (ab)^{-1} = b^{-1}a^{-1}$ (easy to prove)

Examples:

- Let G be a set with an operation $*$ such that
  - G is close under $*$.
  - '$*$' is associative.
  - $\exists\ e \in G$ s.t. $e * x = x\ \forall x \in G$
  - Given $x \in G, \exists\ y$ s.t. $y * x = e$. Show that G is a group.

  Sol: Let $x * e = z \rightarrow y * x * e = y * z = e \$\rightarrow y * x = y * z \rightarrow x = z$

  Let $x * y = z \rightarrow y * x * y = y * z \$\rightarrow y * e = y * z \rightarrow e = z$

- Let G be a **finite** nonempty set with an operation $*$ such that:
  - G is closed under $*$.
  - $*$ is associative.
  - Given $a, b, c, \in G$ with $a * b = a * c$, then $b = c$.
  - Given $a, b, c, \in G$ with $b * a = c * a$, then $b = c$. Show that G is a group.

  Sol: Note that in case of set $\mathbb{N}$ with operation of addition, these properties are satisfied but we know that it doesn't form a group.

  Idea: Reduce this problem to the previous one.

  Existence of Identity, consider the mapping $\Psi_a : G \rightarrow G, \Psi_a(b) = b * a$. Since G is finite and the map is one one, it is onto as well. $\rightarrow \exists\ e_a \in G$ s.t. $e_a * a = a$. (from this it follows that $e_a * e_a * a = e_a * a \rightarrow e_a * e_a = e_a$ and therefore if $a * e\_a = z \rightarrow a * e\_a * e\_a = z * e\_a \$\rightarrow a * e_a = z * e_a \rightarrow a = z$)

  Claim: $\forall\ c \in G, c * e = c$ (Where $e = e_a$)

  As let $c * e = z \rightarrow c * e * a = z * a = c * a \rightarrow z = c$

  Similarly $e * c = c$ and thus uniqueness of identity follows.

  And from map it follows that $\exists\ k, ka = e$ thus inverse of $a = k$, similarly for each element of G.

  Rest is easy from above example.

Dihedral Group

Suppose we remove a square region from a plane, move it in some way, then put the square back into the space it originally occupied. We would like to describe all possible ways in which this can be done. More specifically, we want to describe the possible relationships between the starting position of the square

and its final position in terms of motions. However, we are interested in the net effect of a motion, rather than in the motion itself.

To begin, we can think of the square region as being transparent (glass, say), with the corners marked on one side with the colors blue, white, pink, and green. This makes it easy to distinguish between motions that have different effects.

The eight motions $R_0, R_{90}, R_{180}, R_{270}, H, V, D$, and D', together with the operation composition, form a mathematical system called the dihedral group of order 8. Note: Inverse of R_α, L is $R_{360-\alpha}, L$ resp. (L is a reflection)

To be sure that D_4 is indeed a group, we should check this equation for each of the $8^3 = 512$ possible choices of a, b, and c in D_4. In practice, however, this is rarely done! Here, for example, we simply observe that the eight motions are functions and the operation is function composition. Then, since function composition is associative, we do not have to check the equations.

Cayley Table (i.e. operation table, aka composition table) for D_4

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	H
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

The analysis carried out above for a square can similarly be done for an equilateral triangle or regular pentagon or, indeed, any regular n-gon ($n \geq 3$). The corresponding group is denoted by D_n and is called the dihedral group of order $2n$. It is often called the group of symmetries of a regular n-gon.

A plane symmetry of a figure F in a plane is a function from the plane to itself that carries F onto F and preserves distances; that is, for any points p and q in the plane, the distance from the image of p to the image of q is the same as the distance from p to q.

The symmetry group of a plane figure is the set of all symmetries of the figure. Obviously, a rotation of a plane about a point in the plane is a symmetry of the plane, and a rotation about a line in three dimensions is a symmetry in three-dimensional space. Similarly, any translation of a plane or of three-dimensional space is a symmetry. A reflection across a line L is that function that leaves every point of L fixed and takes any point q, not on L, to the point q' so that L is the perpendicular bisector of the line segment joining q and q'. A reflection across a plane in three dimensions is defined analogously.

Just as a reflection across a line is a plane symmetry that cannot be achieved by a physical motion of the plane in two dimensions, a reflection across a plane

is a three-dimensional symmetry that cannot be achieved by a physical motion of three-dimensional space.

Another Representation of D_n

Let $S = \mathbb{R}^2$ and $n \in \mathbb{N}; n > 2$

Consider,

$f : S \to S$ s.t. $f(x, y) = (-x, y)$

and $h : S \to S$ be a rotation by an angle of $2\pi/n$ in the counterclockwise dirn.

Then $G = \{f^k h^j \mid k = 0, 1 \text{ and } j = 0, 1, ..., n-1\} = D_n$

SubGroups

Definition: (Order of a group) The number of elements of a group (finite or infinite) is called its order. We will use $|G|$ to denote the order of G (Also denoted as $o(G)$).

Definition: (Order of an element) The order of an element g (denoted as $o(h)$) in a group G is the smallest positive integer n such that $g^n = e$. (In additive notation, this would mean $ng = 0$.) If no such integer exists, we say that g has infinite order. The order of an element g is denoted by $|g|$.

Example: Consider U(15) = {1, 2, 4, 7, 8, 11, 13, 14} under multiplication modulo 15. This group has order 8. $|13|$? Soln: Compute $13^1, 13^2, 13^3, 13^4$ to get answer as 4, however there is trick: $13 = -2 \bmod 15 \Rightarrow 13^2 = (-2)^2 = 4, 13^3 = -2 \cdot 4 = -8, 13^4 = (-2)(-8) = 1$.

Example: Consider Z under ordinary addition. Here every nonzero element has infinite order, since the sequence $a, 2a, 3a, ...$ never includes 0 when $a \neq 0$.

Definition: (Subgroup) If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G.

We use the notation $H \leq G$ to mean that H is a subgroup of G. If we want to indicate that H is a subgroup of G but is not equal to G itself, we write $H < G$. Such a subgroup is called a proper subgroup. The subgroup e is called the trivial subgroup of G; a subgroup that is not e is called a nontrivial subgroup of G.

When determining whether or not a subset H of a group G is a subgroup of G, one need not directly verify the group axioms as it will become evident from discussion below.

Theorem 1: (One-Step Subgroup Test) Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G. (In additive notation, if $a - b$ is in H whenever a and b are in H, then H is a subgroup of G.)

Proof: Since the operation of H is the same as that of G, it is clear that this operation is associative. Next, we show that e is in H. Since H is nonempty, we may pick some x in H. Then, letting $a = x$ and $b = x$ in the hypothesis, we have $e = xx^{-1} = ab^{-1}$ is in H. To verify that x^{-1} is in H whenever x is in H, all we need to do is to choose $a = e$ and $b = x$ in the statement of the theorem. Finally, the proof will be complete when we show that H is closed; that is, if

x, y belong to H, we must show that xy is in H also. Well, we have already shown that y^{-1} is in H whenever y is; so, letting $a = x$ and $b = y^{-1}$, we have $xy = x(y^{-1})^{-1} = ab^{-1}$ is in H.

:::tip Tip To apply the above theorem, follow these steps:-

1. Identify the property P that distinguishes the elements of H; that is, identify a defining condition.
2. Prove that the identity has property P. (This verifies that H is nonempty.)
3. Assume that two elements a and b have property P.
4. Use the assumption that a and b have property P to show that ab^{-1} has property P. ::: **Example (easy):** Let G be an Abelian group under multiplication with identity e. Then $H = \{x^2 \mid x \in G\}$ is a subgroup of G. Since $e^2 = e$, the identity has the correct form. Next, we write two elements of H in the correct form, say, a^2 and b^2. We must show that $a^2(b^2)^{-1}$ also has the correct form; that is, $a^2(b^2)^{-1}$ is the square of some element. Since G is Abelian, we may write it as $(ab^{-1})^2$, which is the correct form. Thus, H is a subgroup of G.

- Let H be a subgroup of G. For any fixed x in G, define $xHx^{-1} = \{xhx^{-1} \mid h \in H\}$. Easy to prove that xHx^{-1} is a subgroup of G.

Theorem 2: (Two-Step Subgroup Test) Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H (H is closed under the operation), and a^{-1} is in H whenever a is in H (H is closed under taking inverses), then H is a subgroup of G.

Proof: By Theorem 1, it suffices to show that $a, b \in H$ implies $ab^{-1} \in H$. So, we suppose that $a, b \in H$. Since H is closed under taking inverses, we also have $b^{-1} \in H$. Thus, $ab^{-1} \in H$ by closure under multiplication.

:::note Note 1. Let G be an Abelian group and H and K be subgroups of G. Then $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G. (Easy to show.) 2. Intersection of subgroups is a subgroup (easy to show). :::

How do you prove that a subset of a group is not a subgroup? Here are three possible ways, any one of which guarantees that the subset is not a subgroup:

1. Show that the identity is not in the set.
2. Exhibit an element of the set whose inverse is not in the set.
3. Exhibit two elements of the set whose product is not in the set.

When dealing with finite groups, it is easier to use the following subgroup test.

Theorem 3: (Finite Subgroup Test) Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

Proof: In view of Theorem 2, we need only prove that $a^{-1} \in H$ whenever $a \in H$. If $a = e$, then $a^{-1} = a$ and we are done. If $a \neq e$, consider the sequence $a, a^2, ...$ By closure, all of these elements belong to H. Since H is finite, not all of these elements are distinct. Say $a^i = a^j$ and $i > j$. Then, $a^{i-j} = e$; and since

$a \neq e, i-j > 1$. Thus, $aa^{i-j-1} = a^{i-j} = e$ and, therefore, $a^{i-j-1} = a^{-1}$. But $i-j-1 \geq 1$ implies $a^{i-j-1} \in H$ and we are done. ■

Cyclic Subgroups

For any element a from a group, we let $\langle a \rangle$ denote the set $\{a^n \mid n \in Z\}$. In particular, observe that the exponents of a include all negative integers as well as 0 and the positive integers (a^0 is defined to be the identity). *Clearly it forms a subgroup.* This subgroup is called the cyclic subgroup of G generated by a. In the case that $G = \langle a \rangle$, we say that G is cyclic and a is a generator of G. (A cyclic group may have many generators.) Notice that although the list $..., a^{-2}, a^{-1}, a^0, a^1, a^2, ...$ has infinitely many entries, the set $\{a^n \mid n \in Z\}$ might have only finitely many elements. Also note that, since $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$, every cyclic group is Abelian.

Example: In D_n, the dihedral group of order $2n$, let R denote a rotation of $360/n$ degrees. Then, $R^n = R\_360° = e, R^{n+1} = R, R^{n+2} = R^2, ...$ Similarly, $R^{-1} = R^{n-1}, R^{-2} = R^{n-2}, ...$, so that $\langle R \rangle = \{e, R, ..., R^{n-1}\}$. We see, then, that the powers of R "cycle back" periodically.

For any element a of a group G, it is useful to think of $\langle a \rangle$ as the smallest subgroup of G containing a. This notion can be extended to any collection S of elements from a group G by defining $\langle S \rangle$ as the subgroup of G with the property that $\langle S \rangle$ contains S and if H is any subgroup of G containing S, then H also contains $\langle S \rangle$. Thus, $\langle S \rangle$ is the smallest subgroup of G that contains S. The set $\langle S \rangle$ is called the subgroup generated by S.

Example: in $Z, < 8, 13 >= Z$; in $C, < 1, i >= \{a+bi \mid a, b \in Z\}$ (This group is called the "Gaussian integers"); in R, the group of real numbers under addition, $< 2, \pi, \sqrt{2} >= \{2a + b\pi + c\sqrt{2} \mid a, b, c \in Z\}$; in a group in which a, b, c, and d commute, $< a, b, c, d >= \{a^q b^r c^s d^t \mid q, r, s, t \in Z\}$.

Center of a Group

The center, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. In symbols, $Z(G) = \{a \in G \mid ax = xa$ for all x in G$\}$.

Theorem 4: Center is a Subgroup The center of a group G is a subgroup of G (easy to prove)

Example For $n \geq 3$,

To verify this, first observe that since every rotation in D_n is a power of R_360/n, rotations commute with rotations. We now investigate when a rotation commutes with a reflection. Let R be any rotation in D_n and let F be any reflection in D_n. Observe that since RF is a reflection we have $RF = (RF)^{-1} = F^{-1}R^{-1} = FR^{-1}$. Thus, it follows that R and F commute

if and only if $FR = RF = FR^{-1}$. By cancellation, this holds if and only if $R = R^{-1}$. But $R = R^{-1}$ only when $R = R\_0$ or $R = R\_180$, and R_180 is in D_n only when n is even. So, we have proved that $Z(D_n) = \{R_0\}$ when n is odd and $Z(D\_n) = \{R_0, R\_180\}$ when n is even.

Centralizer of a in G

Let a be a fixed element of a group G. The centralizer of a in G, $C(a)$, is the set of all elements in G that commute with a. In symbols, $C(a) = \{g \in G \mid ga = ag\}$.

Theorem 5: $C(a)$ **Is a Subgroup** (Easy to prove)

Notice that for every element a of a group G, $Z(G) \subseteq C(a)$. Also, observe that G is Abelian if and only if $C(a) = G$ for all a in G.

Example: In D_4, we have the following centralizers: $C(R\_0) = D\_4 = C(R\_180)$,

$C(R\_90) = \{R\_0, R\_90, R\_180, R\_270\} = C(R\_270)$,

$C(H) = \{R\_0, H, R\_180, V\} = C(V)$,

$C(D) = \{R\_0, D, R\_180, D'\} = C(D')$.

Cyclic Groups

Example The set $Z\_n = \{0, 1, ..., n-1\}$ for $n \geq 1$ is a cyclic group under addition modulo n. As it is in the case for group Z, 1 and -1 = n - 1 are generators.

Example $Z\_8 =< 1 >=< 3 >=< 5 >=< 7 >$.

Theorem 4.1: Let G be a group, and let a belong to G. If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order, say, n, then $\langle a \rangle = \{e, a, a^2, ..., a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$. (Easy to prove)

Corollary For any group element a, $|a| = | < a > |$.

Corollary $a^k = e$ Implies That $|a|$ Divides k.

What is important about Theorem 4.1 in the finite case is that it says that multiplication in $< a >$ is essentially done by addition modulo n. That is, if $(i + j) \bmod n = k$, then $a^i a^j = a^k$.

Thus, no matter what group G is, or how the element a is chosen, multiplication in $< a >$ works the same as addition in Z_n whenever $|a| = n$. Similarly, if a has infinite order, then multiplication in $< a >$ works the same as addition in Z, since $a^i a^j = a^{i+j}$ and no modular arithmetic is done. For these reasons, the cyclic groups Z_n and Z serve as prototypes for all cyclic groups, and algebraists say that there is essentially only one cyclic group of each order.

Theorem 4.2: Let a be an element of order n in a group and let k be a positive integer. Then $< a^k >=< a^{gcd(n,k)} >$ and $|a^k| = n/gcd(n, k)$.

Proof: To simplify the notation, let $d = gcd(n, k)$ and let $k = dr$. Since $a^k = (a^d)^r$, we have by closure that $< a^k > \subseteq < a^d >$ *which is infact true for any divisor of k.* By Theorem 0.2 (the gcd theorem), there are integers s and t such that $d = ns + kt$. So, $a^d = a^{ns+kt} = a^{ns}a^{kt} = (a^n)^s(a^k)^t = e(a^k)^t = (a^k)^t \in < a^k >$. This proves $< a^d > \subseteq < a^k >$. So, we have verified that $< a^k >=< a^{gcd(n,k)} >$. We prove the second part of the theorem by showing first that $|a^d| = n/d$ for any divisor d of n. Clearly, $(a^d)^{n/d} = a^n = e$, so that $|a^d| \leq n/d$. On the other hand, if i is a positive integer less than n/d, then $(a^d)^i \neq e$ by definition of $|a|$. ■

Corollory 1: In a finite cyclic group, the order of an element divides the order of the group.

Corollory 2: Let $|a| = n$. Then $< a^i >=< a^j >$ if and only if $gcd(n, i) = gcd(n, j)$, and $|a^i| = |a^j|$ if and only if $gcd(n, i) = gcd(n, j)$.

Corollory 3: Let $|a| = n$. Then $< a >=< a^j >$ if and only if $gcd(n, j) = 1$, and $|a| = | < a^j > |$ if and only if $gcd(n, j) = 1$.

Corollory 4: An integer k in Z_n is a generator of Z_n if and only if $gcd(n, k) = 1$.

The value of Corollary 3 is that once one generator of a cyclic group has been found, all generators of the cyclic group can easily be determined.

Let us use it to find all generators of the cyclic group $U(50)$. First, note that direct computations show that $|U(50)| = 20$ and that 3 is one of its generators. Thus, in view of Corollary 3, the complete list of generators for U(50) is $3 \bmod 50 = 3, 3^3 \bmod 50 = 27, 3^7 \bmod 50 = 37, 3^9 \bmod 50 = 33$, $3^{11} \bmod 50 = 47, 3^{13} \bmod 50 = 23, 3^{17} \bmod 50 = 13, 3^{19} \bmod 50 = 17$

We should keep in mind that Theorem 4.2 and its corollaries apply only to elements of finite order. Also, $U(n)$ need *not* be cyclic in general for example $U(8)$.

Classification of Subgroups of Cyclic Groups

Theorem 4.3

Every subgroup of a cyclic group is cyclic. Moreover, if $| < a > | = n$, then the order of any subgroup of $< a >$ is a divisor of n; and, for each positive divisor k of n, the group $< a >$ has exactly one subgroup of order k—namely, $< a^{n/k} >$.

Proof: Let $G = \langle a \rangle$ and suppose that H is a subgroup of G. We must show that H is cyclic. If it consists of the identity alone, then clearly H is cyclic. So we may assume that $H \neq \{e\}$. We now claim that H contains an element of the form a^t, where t is positive. since $G = \langle a \rangle$, every element of H has the form a^t; and when a^t belongs to H with $t < 0$, then a^{-t} belongs to H also and $-t$ is positive. Thus, our claim is verified. Now let m be the least positive integer such that $a^m \in H$. By closure, $\langle a^m \rangle \subseteq H$. We next claim that $H = \langle a^m \rangle$. To prove this claim, it suffices to let b be an arbitrary member of H and show that b is in $\langle a^m \rangle$. since $b \in G = \langle a \rangle$, we have $ b=a^{k}$ for some k. Now, apply the division algorithm to k and m to obtain integers q and r such that $k = mq + r$ where $0 \leq r < m$. Then $a^k = a^{mq+r} = a^{mq}a^r$, so that $a^r = a^{-mq}a^k$. since $a^k = b \in H$ and $a^{-mq} = (a^m)^{-q}$ is in H also, $a^r \in H$. But, m is the least

positive integer such that $a^m \in H$, and $0 \leq r < m$, so r must be 0. The theorem that every sub- group of a cyclic group is cyclic.

To prove the next portion of the theorem, suppose that $|\langle a \rangle| = n$ and H is any subgroup of $\langle a \rangle$. We have already shown that $H = \langle a^m \rangle$, where m is the least positive integer such that $a^m \in H$. Using $e = b = a^n$ as in the preceding paragraph, we have $n = mq$.

Finally, let k be any positive divisor of n. We will show that $\left\langle a^{n/k} \right\rangle$ is the one and only subgroup of $\langle a \rangle$ of order $ k .$ From Theorem 4.2, we see that $\left\langle a^{n/k} \right\rangle$ has order $n/\gcd(n, n/k) = n/(n/k) = k$. Now let H be any subgroup of $\langle a \rangle$ of order $ k .$ We have already shown above that $H = \langle a^m \rangle$, where m is a divisor of n. Then $m = \gcd(n, m)$ and $k = |a^m| = |a^{\gcd(n,m)}| = n/\gcd(n, m) = n/m$. Thus, $m = n/k$ and $H = \left\langle a^{n/k} \right\rangle$.

Taking the group in Theorem 4.3 to be Z_n and a to be 1, we obtain the following important special case.

Corollary: For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of $ Z_{n}$ of order k ; moreover, these are the only subgroups of Z_n .

Corollary: Only subgroups of $\mathbb{Z}$ are $m\mathbb{Z}$ (i.e. multiples of m). (Can be proved in a similar way)

Examples:

- To find the generators of the subgroup of order 9 in Z_{36}, we observe that $36/9 = 4$ is one generator. To find the others, we have from Corollary 3 of Theorem 4.2 that they are all elements of Z_{36} of the form $4j$, where $\gcd(9, j) = 1$. Thus,

$$\langle 4 \cdot 1 \rangle = \langle 4 \cdot 2 \rangle = \langle 4 \cdot 4 \rangle = \langle 4 \cdot 5 \rangle = \langle 4 \cdot 7 \rangle = \langle 4 \cdot 8 \rangle$$

Let $\phi(1) = 1$, and for any integer $n > 1$, let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n

---

Theorem 4.4: If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$. (Easy to see by above example)

Notice that for a finite cyclic group of order n, the number of elements of order d for any divisor d of n depends only on d. Thus, Z_8, Z_{640}, and Z_{8000} each have $\phi(8) = 4$ elements of order 8.

Corollary: In a finite group, the number of elements of order d is a multiple of $\phi(d)$

Proof: If a finite group has no elements of order d, the statement is true, since $\phi(d)$ divides 0. Now suppose that $a \in G$ and $|a| = d$. By Theorem 4.4, we know that $\langle a \rangle$ has $\phi(d)$ elements of order d. If all elements of order d in G are in $\langle a \rangle$, we are done. So, suppose that there is an element b in G of order d that is not in $\langle a \rangle$. Then, $\langle b \rangle$ also has $\phi(d)$ elements of order d. This means that we have found $2\phi(d)$ elements of order d in G provided that $\langle a \rangle$ and $\langle b \rangle$ have no elements of order d in common. If there is an element c of order d that belongs to both $\langle a \rangle$ and $\langle b \rangle$, then we have $\langle a \rangle = \langle c \rangle = \langle b \rangle$, so that $b \in \langle a \rangle$, which is a contradiction. Continuing in this fashion, we see that the number of elements of order d in a finite group is a multiple of $\phi(d)$.

Converse of Theorem 4.3 is true

I.e., if a group G of finite order n has a unique subgroup for every order $d|n$ then G is cyclic.

Proof: Let $G = \{a_1, a_2, \ldots, a_n\}$, define $H = G$. Then taking any element in H, we compute $|\langle a_i \rangle| (= k$ say), then, since we have unique subgroup of order k, we have $\phi(k)$ such elements in total in G, we will remove such elements from H and continue like this until H becomes empty. Now since order of a subgroup always divides order of the group and the fact that $\sum_{d|n} \phi(d) = n$, we **must** exaust all the divisors of n and thus we will have an element of order n.

Permutation Groups

Although groups of permutations of any nonempty set A of objects exist, we will focus on the case where A is finite. Furthermore, it is customary, as well as convenient, to take A to be a set of the form $\{1, 2, 3, ..., n\}$.

Array form

β of the set $\{1, 2, 3, 4, 5, 6\}$ given by $\beta(1) = 5, \quad \beta(2) = 3, \quad \beta(3) = 1, \quad \beta(4) = 6, \quad \beta(5) = 2, \quad \beta(6) = 4$ is expressed in array form as

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$$

Composition

Consider

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}, \gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$$

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ & \downarrow & & & \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$$

Examples:

- Symmetric Group S_n: Let $A = \{1, 2, ..., n\}$. The set of all permutations of A is called the symmetric group of degree n and is denoted by S_n . Elements of S_n have the form

  $$\alpha = \begin{bmatrix} 1 & 2 & ... & n \\ \alpha(1) & \alpha(2) & ... & \alpha(n) \end{bmatrix}$$

  It is easy to compute the order of S_n. There are n choices of $\alpha(1)$. Once $\alpha(1)$ has been determined, there are $n - 1$ possibilities for $\alpha(2)$ [since α is one-to-one, we must have $\alpha(1) \neq \alpha(2)$]. After choosing $\alpha(2)$, there are

exactly $n-2$ possibilities for $\alpha(3)$. Continuing along in this fashion, we see that S_n has $n(n-1)\cdot\cdot 3\cdot 2\cdot 1 = n!$ elements.

- **Symmetries of a Square**, we associate each motion in D with the permutation of the locations of each 4 of the four corners of a square. For example, if we label the four corner positions as in the figure below and keep these labels fixed for reference, we may describe a 90° counterclockwise rotation by the permutation

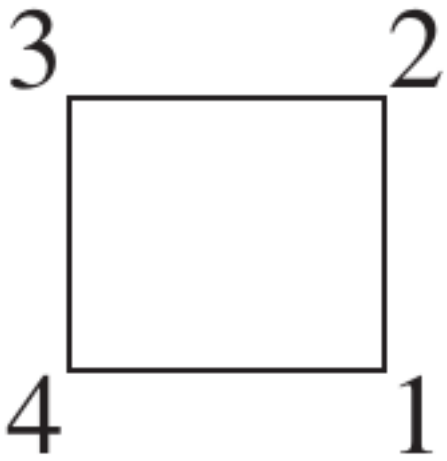

Figure 1: Squre

$$\rho = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$$

whereas a reflection across a horizontal axis yields

$$\phi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$$

These two elements generate the entire group (that is, every element is some combination of the ρ' 's and $\phi' s$).

When D_4 is represented in this way, we see that it is a subgroup of S_4.

Cycle Notation

Consider,

$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$

In cycle notation, β can be written $(2,3,1,5)(6,4)$ or $(4,6)(3,1,5,2)$, since both of these unambiguously specify the function β. An expression of the form $(a_1, a_2, \ldots, a_m)$ is called a cycle of length m or an $m-cycle$.

A multiplication of cycles can be introduced by thinking of a cycle as a permutation that fixes any symbol not appearing in the cycle. Thus, the cycle (4, 6) can be thought of as representing the permutation $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{bmatrix}$.

Let $\alpha = (13)(27)(456)(8)$ and $\beta = (1237)(648)(5)$. (When the domain consists of single-digit integers, it is common practice to omit the commas between the digits.) $\alpha\beta = ?$

Well, keeping in mind that function composition is done from right to left and that each cycle that does not contain a symbol fixes the symbol, we observe that (5) fixes 1; (648) fixes 1; (1237) sends 1 to 2; (8) fixes 2; (456) fixes 2; (27) sends 2 to 7; and (13) fixes 7. So the net effect of $\alpha\beta$ is to send 1 to 7. Thus, we begin $\alpha\beta = (17???)???$. Now, repeating the entire process beginning with 7, and so on, we have $\alpha\beta = (1732)(48)(56)$

Mathematicians prefer not to write cycles that have only one entry. In this case, it is understood that any missing element is mapped to itself. Of course, the identity permutation consists only of cycles with one entry, so we cannot omit all of these! In this case, one usually writes just one cycle. For example, $\varepsilon = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}$ can be written as $\varepsilon = (5)$ or $\varepsilon = (1)$

Theorem 5.1: Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles. (Just give algorithm to find such disjoint cycles)

Theorem 5.2: If the pair of cycles $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$. (easy to prove)

Theorem 5.3: The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Proof: First, observe that a cycle of length n has order n. (easy to see) Next, suppose that α and β are disjoint cycles of lengths m and n, and let k be the least common multiple of m and n. It follows from Theorem 4.1 that both α^k and β^k are the identity permutation ε and, since α and β commute,

$(\alpha\beta)^k = \alpha^k\beta^k$ is also the identity. Thus, we know by Corollary 2 to Theorem 4.1($a^k = e$ implies that $|a|$ divides k) that the order of $\alpha\beta-$ let us call it t -must divide k. But then $(\alpha\beta)^t = \alpha^t\beta^t = \varepsilon$ so that $\alpha^t = \beta^{-t}$. However, it is clear that if α and β have no common symbol, the same is true for α^t and β^{-t}, since raising a cycle to a power does not introduce new symbols. But, if α^t and β^{-t} are equal and have no common symbol, they must both be the identity, because every symbol in α^t is fixed by β^{-t} and vice versa (remember that a symbol not ap- pearing in a permutation is fixed by the permutation). It follows, then, that both m and n must divide t . This means that k , the least common multiple of m and n , divides t also. This shows that $k = t$.

Thus far, we have proved that the theorem is true in the cases where the permutation is a single cycle or a product of two disjoint cycles. The general case involving more than two cycles can be handled in an analogous way.

Examples:

- To determine the orders of the 7! = 5040 elements of S_7, we need only consider the possible disjoint cycle structures of the elements of S_7. For convenience, we denote an n -cycle by (n). Then, arranging all possible disjoint cycle structures of elements of S_7 according to longest cycle lengths left to right, we have

  $(\underline{7})$

  $(\underline{6})(\underline{1})$

  $(\underline{5})(\underline{2})$

  $(\underline{5})(\underline{1})(\underline{1})$

  $(\underline{4})(\underline{3})$

  $(\underline{4})(\underline{2})(\underline{1})$

  $(\underline{4})(\underline{1})(\underline{1})(\underline{1})$

  $(\underline{3})(\underline{3})(\underline{1})$

  $(\underline{3})(\underline{2})(\underline{2})$

  $(\underline{3})(\underline{2})(\underline{1})(\underline{1})$

  $(\underline{3})(\underline{1})(\underline{1})(\underline{1})(\underline{1})$

  $(\underline{2})(\underline{2})(\underline{2})(\underline{1})$

  $(\underline{2})(\underline{2})(\underline{1})(\underline{1})(\underline{1})$

  $(\underline{2})(\underline{1})(\underline{1})(\underline{1})(\underline{1})(\underline{1})$

  $(\underline{1})(\underline{1})(\underline{1})(\underline{1})(\underline{1})(\underline{1})(\underline{1})$

Now, from Theorem 5.3 we see that the orders of the elements of S_7 are 7, 6, 10, 5, 12, 4, 3, 2, and 1.

- We determine the number of elements of S_7 of order 3. By Theorem 5.3, we need only count the number of permutations of the forms $(a_1a_2a_3)$ and $(a_1a_2a_3)(a_4a_5a_6)$. In the first case consider the triple $a_1a_2a_3$. Clearly there are $7 \cdot 6 \cdot 5$ such triples. But this product counts the permutation $(a_1a_2a_3)$ three times (for example, it counts $134, 341, 413$ as distinct triples whereas the cycles $(134), (341)$, and (413) are the same group element). Thus, the number of permutations in S_7 for the form $(a_1a_2a_3)$ is $(7 \cdot 6 \cdot 5)/3 = 70$. For elements of S_7 of the form $(a_1a_2a_3)(a_4a_5a_6)$ there are $(7 \cdot 6 \cdot 5)/3$ ways to create the first cycle and $(4 \cdot 3 \cdot 2)/3$ to create the second cycle but the product of $(7 \cdot 6 \cdot 5)/3$ and $(4 \cdot 3 \cdot 2)/3$ to create the second cycle but the product of $(7 \cdot 6 \cdot 5)/3$ and $(4 \cdot 3 \cdot 2)/3$ counts $(a_1a_2a_3)(a_4a_5a_6)$ and $(a_4a_5a_6)(a_3a_2a_1)$ as distinct when they are equal group elements. Thus, the number of elements in S_7 for the form $(a_1a_2a_3)(a_4a_5a_6)$ is $(7 \cdot 6 \cdot 5)(4 \cdot 3 \cdot 2)/(3 \cdot 3 \cdot 2) = 280$. This gives us 350 elements of order 3 in S_7.

Theorem 5.4: Every permutation in $S_n, n > 1$, is a product of 2 -cycles.

Proof: First, note that the identity can be expressed as $(12)(12)$, and so it is a product of 2-cycles. By Theorem 5.1, we know that every permutation can be written in the form $(a_1a_2 \cdots a_k)(b_1b_2 \cdots b_t) \cdots (c_1c_2 \cdots c_s)$ A direct computation shows that this is the same as

$(a_1a_k)(a_1a_{k-1}) \cdots (a_1a_2)(b_1b_t)(b_1b_{t-1}) \cdots (b_1b_2)$

$\cdots (c_1c_s)(c_1c_{s-1}) \cdots (c_1c_2)$

This completes the proof.

Note: Many authors call two length cycles as transpositions

Lemma: If $\varepsilon = \beta_1\beta_2 \cdots \beta_r$, where the β' s are 2 -cycles, then r is even.

Proof: Clearly, $r \neq 1$, since a 2 -cycle is not the identity. If $r = 2$, we are done. So, we suppose that $r > 2$, and we proceed by induction. Suppose that the rightmost 2 -cycle is (ab). Then, since $(ij) = (ji)$, the product $\beta_{r-1}\beta_r$ can be expressed in one of the following forms shown on the right:

$$\begin{aligned} \varepsilon &= (ab)(ab) \\ (ab)(bc) &= (ac)(ab) \\ (ac)(cb) &= (bc)(ab) \\ (ab)(cd) &= (cd)(ab) \end{aligned}$$

If the first case occurs, we may delete $\beta_{r-1}\beta_r$ from the original product to obtain $\varepsilon = \beta_1\beta_2 \cdots \beta_{r-2}$, and therefore, by the Second Principle of Mathematical Induction, $r-2$ is even. In the other three cases, we replace the form of $\beta_{r-1}\beta_r$ on the right by its counterpart on the left to obtain a new product of \$r \$ 2-cycles that is still the identity, but where the rightmost occurrence of the integer a is in the second-from-the- rightmost 2 -cycle of the product instead of the rightmost 2 -cycle. We now repeat the procedure just described with $\beta_{r-2}\beta_{r-1}$, and, as before, we obtain a product of $(r-2)$ 2 -cycles equal to the identity or a new product of \$r \$ 2-cycles, where the rightmost occurrence of a is in the third 2 -cycle from the right. Continuing this process, we must obtain a product of $(r-2)$ - -cycles equal to the identity, because otherwise we have a product equal to the identity in which the only occurrence of the integer a is in the leftmost 2 -cycle, and such a product does not fix a, whereas the identity does. Hence, by the Second Principle of Mathematical Induction, $r-2$ is even, and r is even as well.

Theorem 5.5: If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of a into a product of 2-cycles must have an even (odd) number of 2-cycles. In symbols, if $\alpha = \beta_1\beta_2 \cdots \beta_r$ and $\alpha = \gamma_1\gamma_2 \cdots \gamma_s$ where the β's and the γ's are 2-cycles, then r and s are both even or both odd.

Proof: Observe that $\beta_1\beta_2 \cdots \beta_r = \gamma_1\gamma_2 \cdots \gamma_s$ implies

$$\begin{aligned} \varepsilon &= \gamma_1\gamma_2 \cdots \gamma_s\beta_r^{-1} \ldots \beta_2^{-1}\beta_1^{-1} \\ &= \gamma_1\gamma_2 \cdots \gamma_s\beta_r \cdots \beta_2\beta_1 \end{aligned}$$

since a 2-cycle is its own inverse. Thus, we have $s + r$ is even. It follows that r and s are both even or both odd.

A permutation that can be expressed as a product of an even number of 2-cycles is called an even permutation. A permutation that can be expressed as a product of an odd number of 2-cycles is called an odd permutation.

Theorem 5.6: The set of even permutations in S_n forms a subgroup of S_n (easy to prove)

The group of even permutations of n symbols is denoted by A_n and is called the alternating group of degree n.

Theorem 5.7: For $n > 1, A_n$ has order $n!/2$

Proof: For each odd permutation α, the permutation $(12)\alpha$ is even and, by the cancellation property in groups, $(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$. Thus, there are at least as many even permutations as there are odd ones. On the other hand, for each even permutation α , the permutation $(12)\alpha$ is odd and $(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$. Thus, there at least as many odd permutations as there are even ones. It follows that there are equal numbers of even and odd permutations. since $|S_n| = n!$, we have $|A_n| = n!/2$

Isomorphism

Group Homomorphism

A homomorphism ϕ from a group G to a group $\overline{G}$ is a mapping from G into $\overline{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all a, b in G.

Isomorphism

Special case of Homomorphism where ϕ (*called as an isomorphism)* is one-to-one and onto. If there is an isomorphism between G onto $\overline{G}$, we say that G and $\overline{G}$ are isomorphic and write $G \approx \overline{G}$.

It is implicit in the definition of isomorphism that isomorphic groups have the same order.

Easy to prove that ϕ^{-1} is as well an isomorphism.

Examples:

- Any infinite cyclic group is isomorphic to Z. Indeed, if a is a generator of the cyclic group, the mapping $a^k \to k$ is an isomorphism. Any finite cyclic group $\langle a \rangle$ of order n is isomorphic to Z_n under the mapping $a^k \to k \bmod n$. That these correspondences are functions and are one-to-one is the essence of Theorem 4.1. Obviously, the mappings are onto and can be verified to be operation preserving.
- $U(10) \approx U(12)$. This is a bit trickier to prove. First, note that $x^2 = 1$ for all x in $U(12)$. Now, suppose that ϕ is an isomorphism from $U(10)$ onto $U(12)$. Then

  $$\phi(9) = \phi(3 \cdot 3) = \phi(3)\phi(3) = 1$$

  and, $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = 1$ Thus, $\phi(9) = \phi(1)$, but $9 \neq 1$, which contradicts the assumption that ϕ is one-to-one.
- There is no isomorphism from Q, the group of rational numbers under addition, to Q^*, the group of nonzero rational numbers under multiplication. If ϕ were such a mapping, there would be a rational number a such

that $\phi(a) = -1$. But then $-1 = \phi(a) = \phi\left(\frac{1}{2}a + \frac{1}{2}a\right) = \phi\left(\frac{1}{2}a\right)\phi\left(\frac{1}{2}a\right) = \left[\phi\left(\frac{1}{2}a\right)\right]^2$ However, no rational number squared is -1

- Any two cyclic group of order m are isomorphic. (easy)

The relation of being isomorphic is an equivalence relation on groups:

- **Reflexivity:** The identity map is an isomorphism from any group to itself.
- **Symmetry:** The inverse of an isomorphism is an isomorphism.
- **Transitivity:** if G is isomorphic to H and H is isomorphic to K, then G is isomorphic to K, via the isomorphism obtained by composing the isomorphisms from G to H and from H to K.

Cayley's Theorem

Theorem 6.1: Every group is isomorphic to a group of permutations.

Proof: To prove this, let G be any group. We must find a group $\overline{G}$ of permutations that we believe is isomorphic to G. Since G is all we have to work with, we will have to use it to construct $\overline{G}$. For any g in G, define a function T_g from G to G by $T_g(x) = gx$ for all x in G. It is easy to see that T_g is a permutation on the of elements of G. Now, let $\overline{G} = \left\{T_g | g \in G\right\}$. Then, $\overline{G}$ is a group under the operation of function composition. To verify this, we first observe that for any g and h in G we have $T_g T_h(x) = T_g\left(T_h(x)\right) = T_g(hx) = g(hx) = (gh)x = T_{gh}(x)$, so that $T_g T_h = T_{gh}$. From this it follows that T_e is the identity and $\left(T_g\right)^{-1} = T_{g^{-1}}$. since function composition is associative, we have verified all the conditions for $\overline{G}$ to be a group.

The isomorphism ϕ between G and $\overline{G}$ is now ready-made. For every g in G, define $\phi(g) = T_g$. If $T_g = T_h$, then $T_g(e) = T_h(e)$ or $ge = he$ Thus, $g = h$ and ϕ is one-to-one. By the way $\overline{G}$ was constructed, we see that ϕ is onto. The only condition that remains to be checked is that ϕ is operation-preserving. To this end, let a and b belong to G. Then $\phi(ab) = T_{ab} = T_a T_b = \phi(a)\phi(b)$

Corollary: Another way to say Cayley's theorem is that, for finite group G, $n = |G|$, there exist a homomorphism $\phi : G \to S_n$ which is injective.

The group $\overline{G}$ constructed previously is called the left regular representation of G.

Properties of Isomorphisms

Theorem 6.2: Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. ϕ carries the identity of G to the identity of $\overline{G}$ (easy to see).
2. For every integer n and for every group element a in $G, \phi(a^n) = [\phi(a)]^n$. (equivalent to saying $\phi(a^{-1}) = \phi(a)^{-1}$ which is easy to see)
3. For any elements a and b in G, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute. (easy to see, thus G is abelian iff $\overline{G}$ is abelian)
4. $G = \langle a \rangle$ if and only if $\overline{G} = \langle \phi(a) \rangle$ (easy… and thus G is cyclic iff $\overline{G}$ is cyclic)
5. $|a| = |\phi(a)|$ for all a in G (isomorphisms preserve orders).
6. For a fixed integer k and a fixed group element b in G, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\overline{G}$. (easy to see, remember that our map is injective)
7. If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order. (follows from 5 and the fact that map is bijective)
8. $\phi(Z(G)) = Z(\overline{G})$ (easy…)
9. If K is a subgroup of G, then $\phi(K) = \{\phi(k) | k \in K\}$ is a subgroup of $\overline{G}$. (easy…)
10. If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{g \in G | \phi(g) \in \overline{K}\}$ is a subgroup of G. (easy…) —

When the group operation is addition, property 2 of Theorem 6.2 is $\phi(na) = n\phi(a)$; property 4 says that an isomorphism between two cyclic groups takes a generator to a generator.

Property 6 is quite useful for showing that two groups are not isomorphic. Often b is picked to be the identity. For example, consider $\mathbf{C}$ and $\mathbf{R}$. Because the equation $x^4 = 1$ has four solutions in $\mathbf{C}$ but only two in $\mathbf{R}$, no matter how one attempts to define an isomorphism from $\mathbf{C}$ to $\mathbf{R}$, property 6 cannot hold.

Automorphism

An isomorphism from a group G onto itself is called an automorphism of G.

Inner Automorphism induced by a

Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all x in G is called the inner automorphism of G induced by a (It is easy to see that it is actually an automorphism of G, it is also denoted as L_a).

When G is a group, we use $Aut(G)$ to denote the set of all automorphisms of G and $Inn(G)$ to denote the set of all inner automorphisms of G.

Theorem 6.3: $Aut(G), Inn(G)$ is a group under the operation of function composition (easy to prove).

Examples: - To determine $\mathrm{Inn}\,(D_4)$, we first observe that the complete list of inner automorphisms is $\phi_{R_0}, \phi_{R_{90}}, \phi_{R_{180}}, \phi_{R_{270}}, \phi_H, \phi_V, \phi_D$, and $\phi_{D'}$. Our job is to determine the repetitions in this list. Since $R_{180} \in Z(D_4)$, we have $\phi_{R_{180}}(x) = R_{180}xR_{180}^{-1} = x$, so that $\phi_{R_{180}} = \phi_{R_0}$. Also, $\phi_{R_{270}}(x) = R_{270}xR_{270}^{-1} = R_{90}R_{180}xR_{180}^{-1}R_{90}^{-1} = R_{90}xR_{90}^{-1} = \phi_{R_{90}}(x)$. Similarly, since $H = R_{180}V$ and $D' = R_{180}D$, we have $\phi_H = \phi_V$ and $\phi_D = \phi_{D'}$ This proves that the previous list can be pared down to $\phi_{R_0}, \phi_{R_{90}}, \phi_H$ and ϕ_D. It can be seen that these are distinct

Evidently, computing $Inn(G)$ is straightforward unlike $Aut(G)$

- To compute Aut (Z_{10}), we try to discover enough information about an element α of Aut (Z_{10}) to determine how α must be defined. Because Z_{10} is so simple, this is not difficult to do. To begin with, observe that once we know $\alpha(1)$, we know $\alpha(k)$ for any k , because it is cyclic and also as $|\alpha(1)| = 10$, we have four candidates for $\alpha(1)$

$$\alpha(1) = 1, \quad \alpha(1) = 3, \quad \alpha(1) = 7, \quad \alpha(1) = 9$$

Now $\alpha_3(a + b) = 3(a + b) = 3a + 3b = \alpha_3(a) + \alpha_3(b)$, we see that α_3 is operation preserving and hence is an automorphism, similarly α_7 and α_9 are also automorphisms.

This gives us the elements of $\mathrm{Aut}\,(Z_{10})$ but not the structure. For instance, what is $\alpha_3\alpha_3$? Well, $(\alpha_3\alpha_3)(1) = \alpha_3(3) = 3 \cdot 3 = 9 = \alpha_9(1)$, so $\alpha_3\alpha_3 = \alpha_9$. Similar calculations show that $\alpha_3^3 = \alpha_7$ and $\alpha_3^4 = \alpha_1$, so that $|\alpha_3| = 4$. Thus, Aut (Z_{10}) is cyclic. Actually, the following Cayley tables reveal that Aut (Z_{10}) is isomorphic to $U(10)$

$U(10)$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

$\mathrm{Aut}\,(Z_{10})$	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_3	α_3	α_9	α_1	α_7
α_7	α_7	α_1	α_9	α_3
α_9	α_9	α_7	α_3	α_1

Theorem 6.5: For every positive integer $n, \mathrm{Aut}\,(Z_n)$ is isomorphic to $U(n)$

Proof: Any automorphism α is determined by the value of $\alpha(1)$, and $\alpha(1) \in U(n)$. Now consider the correspondence from $Aut(Z_n)$ to $U(n)$ given by $T : \alpha \to \alpha(1)$. Clearly it is one - one and onto. To see that it is operation preserving, we have, $T(\alpha\beta) = \alpha(\beta(1)) = \beta(1)\alpha(1) = \alpha(1)\beta(1) = T(\alpha)T(\beta)$.

Cosets and Lagrange's Theorem

Coset of H in G

Let G be a group and let H be a nonempty subset of G. For any $a \in G$, the set $\{ah | h \in H\}$ is denoted by aH. Analogously, $Ha = \{ha | h \in H\}$ and $aHa^{-1} = \left\{aha^{-1} | h \in H\right\}$. When H is a subgroup of G, the set aH (in additive notation $a + H$) is called the left coset of H in G containing a, whereas Ha is called the right coset of H in G containing a. In this case, the element a is called the coset representative of aH (or Ha). We use $|aH|$ to denote the number of elements in the set aH, and $|Ha|$ to denote the number of elements in Ha.

Properties of Cosets

Let H be a subgroup of G, and let a and b belong to G. Then, 1. $a \in aH$. (easy to see) 2. $aH = H$ if and only if $a \in H$. (easy to prove) 3. $(ab)H = a(bH)$ and $H(ab) = (Ha)b$ (easy to prove) 4. $aH = bH$ if and only if $a \in bH$. (easy to prove and thus, any element of a left coset can be used to represent the coset.) 5. $aH = bH$ or $aH \cap bH = \emptyset$ (follows from 4, $ah_1 = bh_2 \rightarrow a = bh_2h_1^{-1} \rightarrow a \in bH$ or alternatively let $c \in aH \cap bH \rightarrow cH = aH = bH$ (from 4)) 6. $aH = bH$ if and only if $b^{-1}a \in H$. (alternate form of 4) 7. $|aH| = |bH|$ (Prove: To prove that $|aH| = |bH|$, it suffices to define a one-to-one mapping from aH onto bH. Obviously, the correspondence $ah \rightarrow bh$ maps aH onto bH. That it is one-to-one follows directly from the cancellation property.)

Corollary: Thus $|aH| = |H|$ as take b to be an element of H.

8. $aH = Ha$ if and only if $H = aHa^{-1}$. (easy to prove)
9. aH is a subgroup of G if and only if $a \in H$. (easy to prove and thus, H itself is the only coset of H that is a subgroup of G)

Note that properties $1, 5$, and 7 of the lemma guarantee that the left cosets of a subgroup H of G partition G into blocks of equal size. Indeed, we may view the cosets of H as a partitioning of G into equivalence classes under the equivalence relation defined by $a \sim b$ if $aH = bH$. (basically if they are in same partition then by 4 we have this)

Examples: - (Use case of property 5) To find the cosets of $H = \{1, 15\}$ in $G = U(32) = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$, we begin with

$H = \{1, 15\}$. We can find a second coset by choosing any element not in H, say 3, as a coset representative. This gives the coset $3H = \{3, 13\}$. We find our next coset by choosing a representative not already appearing in the two previously chosen cosets, say 5. This gives us the coset $5H = \{5, 11\}$. We continue to form cosets by picking elements from $U(32)$ that have not yet appeared in the previous cosets as representatives of the cosets until we have accounted for every element of $U(32)$. We then have the complete list of all distinct cosets of H

- Some authors denote left coset with $H\ G$, and right coset with G/H. Find a bijection from left coset to right coset. **Sol:** Ans is $\psi(aH) = Ha^{-1}$ as $aH = bH \to b^{-1}a \in H \to b^{-1} \in Ha^{-1} \to Hb^{-1} = Ha^{-1}$.

Lagrange's Theorem

Theorem 7.1: If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$.

Proof: Let $a_1H, a_2H, \ldots, a_rH$ denote the distinct left cosets of H in G. Then, for each a in G, we have $aH = a_iH$ for some i . Also, by property 1 of the lemma, $a \in aH$. Thus, each member of G belongs to one of the cosets a_iH. In symbols,

$$G = a_1H \cup \cdots \cup a_rH$$

Now, property 5 of the lemma shows that this union is disjoint, so that

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH| .$$

Finally, since $|a_iH| = |H|$ for each i, we have $|G| = r|H|$

The converse of Lagrange's Theorem is false. For example, a group of order 12 need not have a subgroup of order 6.

The **index** of a subgroup H in G is the number of distinct left cosets of H in G. This number is denoted by $|G : H|$.

Corollary 1: If G is a finite group and H is a subgroup of G, then $|G : H| = |G|/H|$.

Corollary 2: $|a|$ Divides $|G|$

Corollary 3: A group of prime order is cyclic.

Proof: Suppose that G has prime order. Let $a \in G$ and $a \neq e$. Then $|\langle a\rangle|$ divides $|G|$ and $|\langle a\rangle| \neq 1$. Thus, $|\langle a\rangle| = |G|$ and the corollary follows.

Corollary 4: $a^{|G|} = e$

Corollary 5: Fermat's Little Theorem, For every integer a and every prime $p, a^p \bmod p = a \bmod p$ By the division algorithm, $a = pm + r$, where $0 \leq r < p$ Thus, $a \bmod p = r$, and it suffices to prove that $r^p \bmod p = r$. If $r = 0$ the result is trivial, so we may assume that $r \in U(p)$. [Recall that $U(p) = \{1, 2, ..., p-1\}$ under multiplication modulo $p]$ Then, by the preceding corollary, $r^{p-1} \bmod p = 1$ and, therefore, $r^p \bmod p = r$

:::note Note 1. It is relatively easy to prove that if a, m are relatively prime then $a \bmod m (= r), m$ are relatively prime and by similar procedure, we arrive at $r^{\phi(m)} \bmod m = 1$. 2. $U(p)$ for prime p is also denoted as $\mathbb{Z}_p^*$ :::

Theorem 7.2: For two finite subgroups H and K of a group, define the set $HK = \{hk \mid h \in H, k \in K\}$. Then $|HK| = |H||K|/|H \cap K|$.

Proof: Although the set HK has $|H||K|$ products, not all of these products need represent distinct group elements. That is, we may have $hk = h'k'$ where $h \neq h'$ and $k \neq k'$. To determine $|HK|$, we must find the extent to which this happens. For every t in $H \cap K$, the product $hk = (ht)(t^{-1}k)$, so each group element in HK is represented by at least $|H \cap K|$ products in HK. But $hk = h'k'$ implies $t = h^{-1}h' = kk'^{-1} \in H \cap K$, so that $h' = ht$ and $k' = t^{-1}k$. Thus, each element in HK is represented by exactly $|H \cap K|$ products. So, $|HK| = |H||K|/|H \cap K|$.

Examples:

- A group of order 75 can have at most one subgroup of order 25. To see that a group of order 75 cannot have two subgroups of order 25, suppose H and K are two such subgroups. Since $|H \cap K|$ divides $|H| = 25$ and $|H \cap K| = 1$ or 5 results in $|HK| = |H||K|/|H \cap K| = 25 \cdot 25/|H \cap K| =$ 625 or 125 elements, we have that $|H \cap K| = 25$ and therefore $H = K$.

Theorem 7.3: Let G be a group of order $2p$, where p is a prime greater than 2. Then G is isomorphic to Z_{2p} or D_p.

Proof: We assume that G does not have an element of order $2p$ and show that $G \approx D_p$. We begin by first showing that G must have an element of order p. By our assumption and Lagrange's Theorem, any nonidentity element of G must have order 2 or p. Thus, to verify our assertion, we may assume that every nonidentity element of G has order 2 (and thus group is abelian). And thus each element is equal to its inverse. Then, for any nonidentity elements $a, b \in G$ with $a \neq b$, the set $\{e, a, b, ab\}$ is closed and therefore is a subgroup of G of order 4. Since this contradicts Lagrange's Theorem, we have proved that G must have an element of order p; call it a.

Now let b be any element not in $\langle a\rangle$. Then by Lagrange's Theorem and our assumption that G does not have an element of order $2p$, we have that $|b| = 2$ or p. Because $|\langle a\rangle \cap \langle b\rangle|$ divides $|\langle a\rangle| = p$ and $\langle a\rangle \neq \langle b\rangle$ we have that $|\langle a\rangle \cap \langle b\rangle| = 1$. But then $|b| = 2$, for otherwise, by Theorem 7.2 $|\langle a\rangle\langle b\rangle| = |\langle a\rangle||\langle b\rangle| = p^2 > 2p = |G|$, which is impossible. So, any element of G not in $\langle a\rangle$ has order \$ 2 .\$ Next consider ab. Since $ab \notin \langle a\rangle$, our argument above shows that $|ab| = 2$. Then $ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1}$. Moreover, this relation completely determines the multiplication table for G. [For example, $a^3(ba^4) = a^2(ab)a^4 = a^2(ba^{-1})a^4 = a(ab)a^3 = a(ba^{-1})a^3 = (ab)a^2 = (ba^{-1})a^2 = ba$.] since the multiplication table for all noncyclic groups of order $2p$ is uniquely determined by the relation $ab = ba^{-1}$, all noncyclic groups of order $2p$ must be isomorphic to each other. But of course, D_p, the dihedral group of order $2p$, is one such group.

External Direct Products

Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The external direct product of $G_1, G_2, \ldots, G_n$, written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n -tuples for which the i th component is an element of G_i and the operation is componentwise.

In symbols,

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \ldots, g_n) \,|\, g_i \in G_i\}$$

where $(g_1, g_2, \ldots, g_n)\,(g_1', g_2', \ldots, g_n')$ is defined to be $(g_1 g_1', \ g_2 g_2', \ldots, g_n g_n')$. It is understood that each product $g_i g_i'$ is performed with the operation of G_i. Note that in the case that each G_i is finite, we have by properties of sets that $|G_1 \oplus G_2 \oplus \cdots \oplus G_n| = |G_1|\,|G_2| \cdots |G_n|$

It is easy to see that external direct product of groups is itself a group. And external direct product of abelian groups is an abelion group.

If $A \approx_\phi C$, then $A \oplus B \approx C \oplus B$ (easy to see, define $\Phi(a, b) = (\phi(a), b)$)

And $G_1 \oplus G_2 \approx G_2 \oplus G_1$, define $\phi(g_1, g_2) = (g_2, g_1)$.

Examples:

- A group of order 4 is isomorphic to Z_4 or $Z_2 \oplus Z_2$. To verify this, let $G = \{e, a, b, ab\}$. If G is not cyclic, then it follows from Lagrange's Theorem that $|a| = |b| = |ab| = 2$. Then the mapping $e \to (0,0), a \to (1,0)$, $b \to (0,1)$, and $ab \to (1,1)$ is an isomorphism from G onto $Z_2 \oplus Z_2$

Theorem 8.1: The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,

$|(g_1, g_2, \ldots, g_n)| = \operatorname{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$

(Easy to prove)

Examples:

- We determine the number of cyclic subgroups of order 10 in $Z_{100} \oplus Z_{25}$. We begin by counting the number of elements (a, b) of order 10. Possible cases to get LCM 10; (10, 1), ~~(10, 2)~~, (10, 5), ~~(10, 10)~~, ~~(2, 10)~~, ~~(5, 10)~~, (2, 5), ~~(5, 2)~~. That implies answer is $\phi(10) \times 1 + \phi(10) \times \phi(5) + \phi(2) \times \phi(5)$ $= 4 + 4 * 4 + 4 = 24$. Because each cyclic subgroup of order 10 has four elements of order 10 and no two of the cyclic subgroups can have an element of order 10 in common, there must be $24/4 = 6$ cyclic subgroups of order 10.
- For each divisor r of m and s of n, the group $Z_m \oplus Z_n$ has a subgroup isomorphic to $Z_r \oplus Z_s$ (can be proved). To find a subgroup of, say, $Z_{30} \oplus Z_{12}$ isomorphic to $Z_6 \oplus Z_4$, we observe that $< 5 >$ is a subgroup of Z_{30} of order 6 and $< 3 >$ is a subgroup of Z_{12} of order 4, so $< 5 > \oplus < 3 >$ is the desired subgroup.

Theorem 8.2: Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

Proof: Let $|G| = m$ and $|H| = n$, so that $|G \oplus H| = mn$. To prove the first half of the theorem, we assume $G \oplus H$ is cyclic and show that m and n are relatively prime. Suppose that gcd $(m, n) = d$ and (g, h) is a generator of $G \oplus H$. since $(g, h)^{mn/d} = \left((g^m)^{n/d}, (h^n)^{m/d}\right) = (e, e)$, we have $mn = |(g, h)| \leq mn/d$. Thus, $d = 1$

To prove the other half of the theorem, let $G = \langle g \rangle$ and $H = \langle h \rangle$ and suppose $\gcd(m, n) = 1$. Then , $|(g, h)| = \text{lcm}(m, n) = mn = |G \oplus H|$, so that (g, h) is a generator of $G \oplus H$.

Corollary 1: An external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of a finite number of finite cyclic groups is cyclic if and only if $|G_i|$ and $\left|G_j\right|$ are relatively prime when $i \neq j$.

Corollary 2: Let $m = n_1 n_2 \cdots n_k$. Then Z_m is isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ if and only if n_i and n_j are relatively prime when $i \neq j$.

By using the results above in an iterative fashion, one can express the same group (up to isomorphism) in many different forms. For example, we have

$Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_5 \approx Z_2 \oplus Z_6 \oplus Z_5 \approx Z_2 \oplus Z_{30}$

Similarly,

$$\begin{aligned} Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_5 &\approx Z_2 \oplus Z_6 \oplus Z_5 \\ &\approx Z_2 \oplus Z_3 \oplus Z_2 \oplus Z_5 \approx Z_6 \oplus Z_{10} \end{aligned}$$

Thus, $Z_2 \oplus Z_{30} \approx Z_6 \oplus Z_{10}$.

The Group of Units Modulo n as an External Direct Product

If k is a divisor of n, let $U_k(n) = \{x \in U(n) | x \bmod k = 1\}$

It can be readily shown that $U_k(n)$ is indeed a subgroup of $U(n)$.

Theorem 8.3: Suppose s and t are relatively prime. Then,

$U(st) \approx U(s) \oplus U(t)$

Moreover, $U_s(st)$ is isomorphic to $U(t)$ and $U_t(st)$ is isomorphic to $U(s)$

Proof: An isomorphism from $U(st)$ to $U(s) \oplus U(t)$ is $x \to (x \bmod s, x \bmod t)$ (one-one and onto follows from Chinese Remainder Theorem, operation preserving is clear; an isomorphism from $U_s(st)$ to $U(t)$ is $x \to x \bmod t$; an isomorphism from $U_t(st)$ to $U(s)$ is $x \to x \bmod s$. We leave the verification that these mappings are operation-preserving, one-to-one, and onto to the reader.

Corollary: Let $m = n_1 n_2 \cdots n_k$, where $gcd\left(n_i, n_j\right) = 1$ for $i \neq j$. Then $U(m) \approx U\left(n_1\right) \oplus U\left(n_2\right) \oplus \cdots \oplus U\left(n_k\right)$.

Normal Subgroups and Factor Groups

Normal Subgroup

A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all a in G. We denote this by $H \lhd G$.

Theorem 9.1: (Normal Subgroup Test) A subgroup H of G is normal in G if and only if $xHx^{-1} \subseteq H$ for all x in G. (Weaker version of what was shown in 7th chapter)

Proof: Converse is only required to be proved. Consider any $h \in H \rightarrow x^{-1}hx(= b \text{ say }) \in H \rightarrow xbx^{-1} \in xHx^{-1} \rightarrow h \in xHx^{-1}$

A group is called Hamiltonian if it is non-abelian and all its subgroups are normal.

Examples:

Unless proof is given, assume it was easy

- If every left coset is a right coset, then $H \lhd G$.
  Proof: $aH = Hb \rightarrow a \in Hb \rightarrow ab^{-1} \in H \rightarrow Ha = Hb$.
- Every subgroup of an Abelian group is normal.
  - But the converse is not true as consider for example Quaternion group $Q_8 = \langle \overline{e}, i, j, k \mid \overline{e}^2 = e, i^2 = j^2 = k^2 = ijk = \overline{e} \rangle$ where e is the identity element and $\overline{e}$ commutes with the other elements of the group (can be derived). All its subgroups are $\{e\}, \{e, \overline{e}\}, \{e, \overline{e}, i, \overline{e}i\}, \{e, \overline{e}, j, \overline{e}j\}, \{e, \overline{e}, k, \overline{e}k\}, Q_8$ all of which are normal (easy to verify).
- The center $Z(G)$ of a group is always normal.
- The alternating group A_n of even permutations is a normal subgroup of S_n.
- Every subgroup of D_n consisting solely of rotations is normal in D_n.
- Let H be a normal subgroup of a group G and K be any subgroup of G. Then $HK = \{hk | h \in H, k \in K\}$ is a subgroup of G.

- If a group G has a unique subgroup H of some finite order, then H is normal in G. To see that this is so, observe that for any $g \in G, gHg^{-1}$ is a subgroup of G and $|gHg^{-1}| = |H|$.
- Let G be a finite group, $|G| = pm$ where p is a prime and $p \nmid m$ and $H \lhd G$ of order p. Show that for any autmorphism $\phi : G \to G, \phi(H) = H$ (easy, if $\phi(H) \neq H \to \because \phi(H) \cap H = \{e\}$, $H\phi(H)$ is a subgroup of order $p^2 \Rightarrow\Leftarrow$)

Factor Groups or Quotient Groups

Theorem 9.2: Let G be a group and let H be a normal subgroup of G. The set $G/H = \{aH | a \in G\}$ is a group under the operation $(aH)(bH) = abH$ (easy to prove)

Proof: Group axioms are easy to verify but we must verify that the function is well defined, so we need to check whether single element gets map to exactly one element, so consider $a, a', b, b' \in G$ and $aH = a'H, bH = b'H$ to show $abH = a'b'H$ i.e. to show $ab \in a'b'H$, $a = a'h_1, b = b'h_2, ab = a'h_1b'h_2 = a'b'h_3h_2$

Converse of Theorem 9.2 is also true; that is, if the correspondence $aHbH = abH$ defines a group operation on the set of left cosets of H in G, then H is normal in G.

It is crucial to understand that when we factor out by a normal subgroup H, what we are essentially doing is defining every element in H to be the identity.

Also remember that the order of the factor group is $|G|/|H|$

Examples:

- Let $4Z = \{0, \pm 4, \pm 8, ...\}$. To construct $Z/4Z$, we first must determine the left cosets of $4Z$ in Z. Which are

  $0 + 4Z = 4Z = \{0, \pm 4, \pm 8, ...\}$

  $1 + 4Z = \{1, 5, 9, ... ; -3, -7, -11, ...\}$

  $2 + 4Z = \{2, 6, 10, ... ; -2, -6, -10, ...\}$

  $3 + 4Z = \{3, 7, 11, ... ; -1, -5, -9, -9, ...\}$

  Cayley's table

	$0+4Z$	$1+4Z$	$2+4Z$	$3+4Z$
$0+4Z$	$0+4Z$	$1+4Z$	$2+4Z$	$3+4Z$
$1+4Z$	$1+4Z$	$2+4Z$	$3+4Z$	$0+4Z$
$2+4Z$	$2+4Z$	$3+4Z$	$0+4Z$	$1+4Z$
$3+4Z$	$3+4Z$	$0+4Z$	$1+4Z$	$2+4Z$

Clearly, then, $Z/4Z \approx Z_4$. More generally, if for any $n > 0$ we let $nZ = \{0, \pm n, \pm 2n, \pm 3n, ...\}$, then Z/nZ is isomorphic to Z_n

- It can be shown that every finite Abelian group is isomorphic to a direct product of cyclic groups. In particular, an Abelian group of order 8 is isomorphic to one of $Z_8, Z_4 \oplus Z_2$, or $Z_2 \oplus Z_2 \oplus Z_2$. In the next two examples, we examine Abelian factor groups of order 8 and determine the isomorphism type of each.
  - Let $G = U(32) = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$ and $H = U_{16}(32) = \{1, 17\}$. Then G/H is an Abelian group of order $16/2 = 8$. Which of the three Abelian groups of order 8 is it—$Z_8, Z_4 \oplus Z_2, Z_2 \oplus Z_2 \oplus Z_2$? To answer this question, we need only determine the elements of G/H and their orders. Observe that the eight cosets $1H = \{1, 17\}$, $3H = \{3, 19\}, 5H = \{5, 21\}, 7H = \{7, 23\}$ $9H = \{9, 25\}$, $11H = \{11, 27\}, 13H = \{13, 29\}$, and $15H = \{15, 31\}$

    are all distinct, so that they form the factor group G/H. Clearly, $(3H)^2 = 9H \neq H$, and so $3H$ has order at least 4. Thus, G/H is not $Z_2 \oplus Z_2 \oplus Z_2$. On the other hand, direct computations show that both $7H$ and $9H$ have order 2, so that G/H cannot be Z_8 either, since a cyclic group of even order has exactly one element of order 2 (Theorem 4.4) . This proves that $U(32)/U_{16}(32) \approx Z_4 \oplus Z_2$, which (not so incidentally!) is isomorphic to $U(16)$.
  - Let $G = U(32)$ and $K = \{1, 15\}$. Then $|G/K| = 8$ and we ask, which of the three Abelian groups of order 8 is G/K? Since $(3K)^4 = 81K = 17K \neq K, |3K| = 8$. Thus, $G/K \approx Z_8$
- If H has index 2 in G, then H is normal in G. **Proof:** Let $a \notin H \rightarrow aH \neq H$ and $Ha \neq H$ but since we only have two cosets $\rightarrow aH = Ha$.

Applications of Factor Groups

- The group A_4 of even permutations on the set $\{1, 2, 3, 4\}$ has no subgroup H of order 6. To see this, suppose that A_4 does have a subgroup H of order 6. By above example, we know that $H \lhd A_4$. Thus, the factor group A_4/H exists and has order 2. We have for all $\alpha \in A_4$ that $\alpha^2 H = (\alpha H)^2 = H$. Thus, $\alpha^2 \in H$ for all $\alpha \in A_4$. Referring to the main diagonal of the group table for A_4 however, we observe that A_4 has nine different elements of the form α^2, all of which must belong to H, a subgroup of order 6. This is clearly impossible, so a subgroup of order 6 cannot exist in A_4.

Theorem 9.3: Let G be a group and let $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, then G is Abelian.

Proof: Since G is Abelian is equivalent to $Z(G) = G$, it suffices to show that the only element of $G/Z(G)$ is the identity coset $Z(G)$. To this end, let $G/Z(G) = \langle gZ(G)\rangle$ and let $a \in G$. Then there exists an integer i such that $aZ(G) = (gZ(G))^i = g^iZ(G)$. Thus, $a = g^iz$ for some z in $Z(G)$. Since both g^i and z belong to $C(g)$, so does a . Because a is an arbitrary element of G this means that every element of G commutes with g so $g \in Z(G)$. Thus, $gZ(G) = Z(G)$ is the only element of $G/Z(G)$.

A few remarks about Theorem 9.3 are in order. First, our proof shows that a better result is possible: If G/H is cyclic, where H is a subgroup of $Z(G)$, then G is Abelian. Second, in practice, it is the contrapositive of the theorem that is most often used—that is, if G is non-Abelian, then $G/Z(G)$ is not cyclic. For example, it follows immediately from this statement and Lagrange's Theorem that a non-Abelian group of order pq, where p and q are primes, must have a trivial center (suppose center is not trivial, that implies its order is either p or q. Say it is $p \rightarrow$ order of $G/Z(G) = q$ and hence it must be cyclic. Third, if $G/Z(G)$ is cyclic, it must be trivial.

Theorem 9.4: For any group G, $G/Z(G)$ is isomorphic to $Inn(G)$.

Proof: Consider the correspondence from $G/Z(G)$ to $Inn(G)$ given by $T : gZ(G) \rightarrow \phi_g$. We can now easily show that it is well defined and as well satisfies properties for it being isomorphism. For one-one, note that $g_1xg_1^{-1} = g_2xg_2^{-1} \rightarrow (g_2^{-1}g_1)x = x(g_2^{-1}g_1)$ thus $g_1 = g_2z, z \in Z(G)$.

Examples: - We know that $|Z(D_6)| = 2$. Thus, $|D_6/Z(D_6)| = 6$. So, by our classification of groups of order 6 (Theorem 7.3), we know that $Inn(D_6)$ is isomorphic to D_3 or Z_6. Now, if $Inn(D_6)$ were cyclic, then, by Theorem 9.4, $D_6/Z(D_6)$ would be also. But then, Theorem 9.3 would tell us that D_6 is Abelian. So, $Inn(D_6)$ is isomorphic to D_3.

Theorem 9.5: (Cauchy's Theorem for Abelian Groups) Let G be a finite Abelian group and let p be a prime that divides the order of G. Then G has an element of order p.

Proof: Clearly, this statement is true for the case in which G has order 2. We prove the theorem by using the Second Principle of Mathematical Induction on $|G|$. That is, we assume that the statement is true for all Abelian groups with fewer elements than G and use this assumption to show that the statement is true for G as well. Certainly, G has elements of prime order, for if $|x| = m$ and $m = qn$, where q is prime, then $|x^n| = q$. So let x be an element of G of some prime order q, say. If $q = p$, we are finished; so assume that $q \neq p$. Since

every subgroup of an Abelian group is normal, we may construct the factor group $\overline{G} = G/ < x >$. Then $\overline{G}$ is Abelian and p divides $|\overline{G}|$, since $|\overline{G}| = |G|/q$. By induction, then, $\overline{G}$ has an element—call it $y < x >$—of order p. Then, $(y < x >)^p = y^p < x >=< x >$ and therefore $y^p \in < x >$. If $y^p = e$, we are done. If not, then y^p has order q and y^q has order p.

Internal Direct Products

We say that G is the internal direct product of H and K and write $G = H \times K$ if H and K are normal subgroups of G and $G = HK$ and $H \cap K = \{e\}$.

Let $H_1, H_2, ..., H_n$ be a finite collection of normal subgroups of G. We say that G is the internal direct product of $H_1, H_2, ..., H_n$ and write $G = H_1 \times H_2 \times ... \times H_n$, if 1. $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n | h_i \in H_i\}$ 2. $(H_1 H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ for $i = 1, 2, ..., n-1$

:::note Note Condition 2 above will guarantee for $i \neq j, H_i \cap H_j = \{e\}$ as wlog assume $j > i$ then by making other h_k as e we get using $(H_1 H_2 \cdots H_i \cdots H_{j-1}) \cap H_j = \{e\}, H_i \cap H_j = \{e\}$ :::

Theorem 9.6: $H_1 \times H_2 \times \cdots \times H_n \approx H_1 \oplus H_2 \oplus \cdots \oplus H_n$

Proof: We first show that the normality of the H's together with the second condition of the definition guarantees that h's from different H_i's commute. We have $h_i h_j = h_j h_i' = h_j' h_i \rightarrow h_j'^{-1} h_j = h_i h_i'^{-1} \rightarrow h_j'^{-1} h_j = e \rightarrow h_j = h_j'$...

Similarly we can easily prove that each member of G can be expressed uniquely in the form $h_1 h_2 \cdots h_n$, where $h_i \in H_i$.

We may now define a function ϕ from G to $H_1 \oplus H_2 \oplus \cdots \oplus H_n$ by $f(h_1 h_2 \cdots h_n) = (h_1, h_2, ..., h_n)$. Which is easily verifiable to be an isomorphism.

Theorem 9.7: Every group of order p^2, where p is a prime, is isomorphic to Z_{p^2} or $Z_p \oplus Z_p$

Proof: Let G be a group of order p^2, where p is a prime. If G has an element of order p^2, then G is isomorphic to Z_{p^2}. So, by Corollary 2 of Lagrange's Theorem, we may assume that every nonidentity element of G has order p.

First we show that for any element a, the subgroup $< a >$ is normal in G. If this is not the case, then there is an element b in G such that bab^{-1} is not in $< a >$. Then $< a >$ and $< bab^{-1} >$ are distinct subgroups of order p. Since $< a > \cap < bab^{-1} >$ is a subgroup of both $< a >$ and $< bab^{-1} >$, we have that $< a > \cap < bab^{-1} >= \{e\}$. From this it follows that the distinct left cosets of $< bab^{-1} >$ are $< bab^{-1} >, a < bab^{-1} >, a^2 < bab^{-1} >, \ldots, a^{p-1} < bab^{-1} >$ (as if $a^i \in a^j\langle bab^{-1}\rangle \rightarrow a^{i-j} \in \langle bab^{-1}\rangle$). Since b^{-1} must lie in one of these cosets, we may write b^{-1} in the form $b^{-1} = a^i(bab^{-1})^j = a^iba^jb^{-1}$ for some i and j. Canceling the b^{-1} terms, we obtain $e = a^iba^j$ and therefore $b = a^{-i-j} \in < a >$. This contradiction verifies our assertion that every subgroup of the form $< a >$ is normal in G. To complete the proof, let x be any nonidentity element in G and y be any element of G not in $< x >$. Then, by comparing orders and using Theorem 9.6, we see that $G =< x > \times < y > \approx Z_p \oplus Z_p$.

Corollary: If G is a group of order p^2, where p is a prime, then G is Abelian.

Note: Indian authors seems to switch the notation for EDP and IDP.

It follows directly from Theorem 8.3, its corollary, and Theorem 9.6 that if $m = n_1n_2\cdots n_k$, where $gcd(n_i, n_j) = 1$ for $i \neq j$, then

$U(m) = U_{m/n_1}(m) \times U_{m/n_2}(m) \times \cdots U_{m/n_k}(m)$

$\approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k)$.

:::note Note $U_{m/n_i}(m) \cap U_{m/n_j}(m) = \{e\}\ \forall i \neq j$ as $x = mk/n_1 + 1 = mk'/n_2 + 1 \rightarrow n_1k' = n_2k \rightarrow k' = n_2, k = n_1 \rightarrow x = m + 1$ which is absurd. :::

Group Homomorphisms and Class Equation

When defining a homomorphism from a group in which there are several ways to represent the elements, caution must be exercised to ensure that the correspondence is a function.

Kernal of a Homomorphism

The kernel of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G \mid \phi(x) = e\}$. The kernel of ϕ is denoted by $\operatorname{Ker}\phi$ and clearly it forms a subgroup.

The kernel of an isomorphism is the trivial subgroup.

Relation with linear algebra: Every linear transformation is a group homomorphism and the null-space is the same as the kernel. An invertible linear transformation is a group isomorphism.

Properties of Homomorphisms

Theorem 10.1: Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let g be an element of G and let H be a subgroup of G. Then 1. ϕ carries the identity of G to the identity of $\overline{G}$. 2. $\phi(g^n) = (\phi(g))^n$ for all n in Z. 3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$. (easy) 4. $\phi(a) = \phi(b)$ if and only if $a\operatorname{Ker}\phi = b\operatorname{Ker}\phi$. (easy) 5. If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\operatorname{Ker}\phi$. (easy, $g\operatorname{Ker} \subseteq \phi^{-1}(g')$ is straight forward, and other dirn follows from above) 6. $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of $\overline{G}$. (easy) 7. If H is cyclic, then $\phi(H)$ is cyclic. (easy) 8. If H is Abelian, then $\phi(H)$ is Abelian. (easy) 9. If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$. (easy) 10. If $|\operatorname{Ker}\phi| = n$, then ϕ is an n-to-1 mapping from G onto $\phi(G)$ (From 4 or 5 we see that $a \in b\operatorname{Ker}\phi$ Now $|b\operatorname{Ker}\phi| = n$. So $|\phi(G)| \cdot |\operatorname{Ker}\phi| = |G|$) 11. If $|H| = n$, then $|\phi(H)|$ divides n. (let ϕ_H denote the restriction of ϕ to the elements of H. Then ϕ_H is a homomorphism from H onto $\phi(H)$. Suppose $|\operatorname{Ker}\phi_H| = t$. Then, by property 5, ϕ_H is a t-to-1 mapping. So, $|\phi(H)|t = |H|$. 12. If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a subgroup of G. (easy..) 13. If $\overline{K}$ is a normal

subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G \mid \phi(k) \in \overline{K}\}$ is a normal subgroup of G. (easy..) (As a **Corollary**, $\operatorname{Ker}\phi$ is a normal subgroup of G. (take $\overline{K}$ as $\{e\}$). *Note:* As we will soon see, converse is as well true) 14. If ϕ is onto and $\operatorname{Ker}\phi = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$.

Examples:

- Let G be a finite abelian group, define $\phi_m : G \to G, \phi_m(g) = g^m$, when is ϕ_m an automorphism? **Sol:** Since we are interested in automorphism, just checking whether map is one - one, is enough. Now map is one - one iff $\operatorname{Ker}(\phi) = \{e\}$, sufficient condition for that is $(m, |G|) = 1$. As suppose $\operatorname{Ker}(\phi) \neq \{e\}$, $\to \exists\ g \in G$ s.t. $g^m = e \to o(g)|m$ but $(o(g), |G|) = 1 \Rightarrow\Leftarrow$.
- Consider the mapping ϕ from $\mathbb{C}$ to $\mathbb{C}$ given by $\phi(x) = x^4$. Since $(xy)^4 = x^4y^4$, ϕ is a homomorphism. Clearly, $\operatorname{Ker}\phi = \{x \mid x^4 = 1\} = \{1, -1, i, -i\}$. So, we know that ϕ is a 4-to-1 mapping. Now let's find all elements that map to, say, 2. Certainly, $\phi(\sqrt[4]{2}) = 2$. Then, the set of all elements that map to 2 is $\{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i\}$
- We determine all homomorphisms from Z_{12} to Z_{30}. By property 2 of Theorem 10.1, such a homomorphism is completely specified by the image of 1. That is, if 1 maps to a, then x maps to xa. Lagrange's Theorem and property 3 of Theorem 10.1 require that $|a|$ divide both 12 and 30. So, $|a| = 1$, 2, 3, or 6. Thus, $a = 0$, 15, 10, 20, 5, or 25. This gives us a list of candidates for the homomorphisms. That each of these six possibilities yields an operation-preserving, well defined function can now be verified by direct calculations.

Theorem 10.2: (First Isomorphism Theorem) Let ϕ be a group homomorphism from G to $\overline{G}$. Then the mapping from $G/\operatorname{Ker}\phi$ to $\phi(G)$, given by $g\operatorname{Ker}\phi \to \phi(g)$, is an isomorphism. In symbols, $G/\operatorname{Ker}\phi \approx \phi(G)$. (function definition is valid, one-one follows from property 4 discussed above and onto is easy to see, operation preserving can be easily verified)

Corollary: If ϕ is a homomorphism from a finite group G to $\overline{G}$, then $|\phi(G)|$ divides $|G|$ and $|\overline{G}|$.

Examples:

- $Z/\langle n\rangle \approx Z_n$
- (N/C **Theorem**) Let H be a subgroup of a group G. Normalizer of H in G is $N(H) = \{x \in G \mid xHx^{-1} = H\}$ and the centralizer of H in G is $C(H) = \{x \in G \mid xhx^{-1} = h\ \forall h \in H\}$. Consider the mapping from $N(H)$ to $Aut(H)$ given by $g \to \phi_g$, where ϕ_g is the inner automorphism of H

induced by g. This mapping is a homomorphism with kernel $C(H)$. So, by Theorem 10.2, $N(H)/C(H)$ is isomorphic to a subgroup of $Aut(H)$.

- Let G be a group of order 35, we will show that it is cyclic. By Lagrange's Theorem, every nonidentity element of G has order 5, 7, or 35. If some element has order 35, G is cyclic. So we may assume that all nonidentity elements have order 5 or 7. However, not all such elements can have order 5, since elements of order 5 come 4 at a time (if $|x| = 5$, then $|x^2| = |x^3| = |x^4| = 5$) and 4 does not divide 34. Similarly, since 6 does not divide 34, not all nonidentity elements can have order 7. So, G has elements of order 7 and order 5. Since G has an element of order 7, it has a subgroup of order 7. Let us call it H. In fact, H is the only subgroup of G of order 7, for if K is another subgroup of G of order 7, we have by Theorem 7.2 that $|HK| = |H||K|/|H \cap K| = 7 \cdot 7/1 = 49$ (Intersection is $\{e\}$ because each element is a generator). But, of course, this is impossible in a group of order 35. Since for every a in G, aHa^{-1} is also a subgroup of G of order 7 (easy to prove), we must have $aHa^{-1} = H$. So, $N(H) = G$. Since H has prime order, it is cyclic and therefore Abelian. In particular, $C(H)$ contains H. So, 7 divides $|C(H)|$ and $|C(H)|$ divides 35. It follows, then, that $C(H) = G$ or $C(H) = H$. If $C(H) = G$, then we may obtain an element x of order 35 by letting $x = hk$ (since order of h, k is relatively prime and they commute, therefore order of $x = |h||k|$), where h is a nonidentity element of H and k has order 5. On the other hand, if $C(H) = H$, then $|C(H)| = 7$ and $|N(H)/C(H)| = 35/7 = 5$. However, 5 does not divide $|Aut(H)| = |Aut(Z_7)| = 6$. This contradiction shows that G is cyclic.

Theorem 10.3: Every normal subgroup of a group G is the kernel of a homomorphism of G. In particular, a normal subgroup N is the kernel of the mapping $g \to gN$ from G to G/N.

Proof: Define $\gamma : G \to G/N$ by $\gamma(g) = gN$. (This mapping is called the natural homomorphism from G to G/N.) Then, $\gamma(xy) = (xy)N = xNyN = \gamma(x)\gamma(y)$. Moreover, $g \in \operatorname{Ker}\gamma$ if and only if $gN = \gamma(e) = N$, which is true if and only if $g \in N$.

Examples:

- If G is a group of order 60 and G has a homomorphic image of order 12 that is cyclic (as it is cyclic, it is normal and thus its inverse will also be normal subgroup, also since it is cyclic, it has normal subgroups of order 1, 2, 3, 4, 6, 12), then G has normal subgroups of orders 5, 10, 15, 20, 30, and 60 (property 10).
- Suppose we are asked to find an infinite group that is the union of three proper subgroups. Instead of attempting to do this directly, we first make

the problem easier by finding a finite group that is the union of three proper subgroups. Observing that $Z_2 \oplus Z_2$ is the union of $H_1 = \langle 1, 0\rangle, H_2 = \langle 0, 1\rangle$, and $H_3 = \langle 1, 1\rangle$, we have found our finite group. Now all we need do is think of an infinite group that has $Z_2 \oplus Z_2$ as a homomorphic image and pull back H_1, H_2, and H_3, and our original problem is solved. Clearly, the mapping from $Z_2 \oplus Z_2 \oplus Z$ onto $Z_2 \oplus Z_2$ given by $\phi(a, b, c) = (a, b)$ is such a mapping, and therefore $Z_2 \oplus Z_2 \oplus Z$ is the union of $\phi^{-1}(H_1) = \{(a, 0, c,) \mid a \in Z_2, c \in Z\}, \phi^{-1}(H_2) = \{(0, b, c) \mid b \in Z_2, c \in Z\}$, and $\phi^{-1}(H_3) = \{(a, a, c) \mid a \in Z_2, c \in Z\}$.

Class Equation

CE for D_n:

$D_n = \{r^i\rho^j \mid i \in \{0, 1\}, j \in \{0, 1, ..., n-1\}\}$

Consider any rotation ρ^i, we have:- * $\rho^j\rho^i\rho^{-j} = \rho^i$ * $r\rho^j\rho^i\rho^{-j}r = \rho^{-i}$ ($r\rho = \rho^{-1}r \rightarrow r\rho^k r = \rho^{-k}$)

Thus conjugacy classes containing ρ^i are of the form $\{\rho^i, \rho^{-i}\}$.

- If n is odd, we have $|\{e, \rho, \rho^2, ..., \rho^{n-1}\}| = 1 + \underbrace{2 + 2 + ... + 2}_{(n-1)/2 \text{ times}}$.
- o/w we have $1 + 1 + \underbrace{2 + ... + 2}_{(n-2)/2 \text{ times}}$.

Now consider any reflection $r\rho^i$. * $\rho^j r\rho^i\rho^{-j} = r\rho^{i-2j} = r\rho^i\rho^{-2j}$. Now $\langle\rho^{-2j}\rangle = \langle\rho^{2j}\rangle = \langle\rho^2\rangle = \langle\rho^{gcd(2,n)}\rangle$ * In case n is odd, this is equal to $\langle\rho\rangle$, thus all remaining elements belong to this conjugacy class. * $r\rho^j r\rho^i\rho^{-j}r = r\rho^{2j-i} = r\rho^{-i}\rho^{2j}$. * In case n is even, $gcd(2, n) = 2$ and notice that $r\rho^i\langle\rho^2\rangle = r\rho^{-i}\langle\rho^2\rangle$. * As if i is odd, $\rho^{-i} = \rho^{n-i} = \rho^{odd}$, similarly for other case. * Thus for even n we have two conjugacy classes, $\{r\rho^{odd}\}$ and $\{r\rho^{even}\}$ each of size $n/2$.

Introduction to Rings

A ring R is a set with two binary operations, addition (denoted by $a + b$) and multiplication (denoted by ab), such that for all a, b, c in R:

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. There is an additive identity 0. That is, there is an element 0 in R such that $a + 0 = a$ for all a in R.
4. There is an element $-a$ in R such that $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

So, a ring is an Abelian group under addition, also having an associative multiplication that is left and right distributive over addition. Note that multiplication need not be commutative. When it is, we say that the ring is commutative. Also, a ring need not have an identity under multiplication. A unity (or identity) in a ring is a nonzero element that is an identity under multiplication. A nonzero element of a commutative ring with unity need not have a multiplicative inverse. When it does, we say that it is a unit of the ring. Thus, a is a unit if a^{-1} exists.

The following terminology and notation are convenient. If a and b belong to a commutative ring R and a is nonzero, we say that a divides b (or that a is a factor of b) and write $a|b$, if there exists an element c in R such that $b = ac$. If a does not divide b, we write $a \nmid b$.

Recall that if a is an element from a group under the operation of addition and n is a positive integer, na means $a + a + \cdots + a$, where there are n summands. When dealing with rings, this notation can cause confusion, since we also use juxtaposition for the ring multiplication. When there is the potential for confusion, we will use $n \cdot a$ to mean $a + a + \cdots + a$ (n summands).

We use $b - c$ to denote $b + (-c)$.

If a, b, and c belong to a ring, $a \neq 0$ and $ab = ac$, we cannot conclude that $b = c$. Similarly, if $a^2 = a$, we cannot conclude that $a = 0$ or 1

- Show that if m and n are integers and a and b are elements from ring, then $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$. **Sol:** $(m \cdot a)(n \cdot b) = (a+a+\cdots+a)(b+b+\cdots+b) =$

$(ab + ab + \cdots + ab)$, where the last term has mn summands.

- Note that since R is an abelian group under addition, every subgroup of it is normal.

Subrings

A subset S of a ring R is a subring of R if S is itself a ring with the operations of R.

Theorem 11.3: A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication—that is, if $a - b$ and ab are in S whenever a and b are in S. (easy…)

Examples:

- $\{0\}$ and R are subrings of any ring R. $\{0\}$ is called the trivial subring of R.
- $\{0, 2, 4\}$ is a subring of the ring Z_6, the integers modulo 6. Note that although 1 is the unity in Z_6, 4 is the unity in $\{0, 2, 4\}$ and can be verified that it is a field (defined later).
- The set of Gaussian integers $Z[i] = \{a + bi \mid a, b \in Z\}$ is a subring of the complex numbers $\mathbb{C}$.
- For each positive integer n, the set $nZ = \{0, \pm n, \pm 2n, \pm 3n, ...\}$ is a subring of the integers Z.

Example: Let $R_1, R_2, ..., R_n$ be rings. We can use these to construct a new ring as follows. Let $R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(a_1, a_2, ..., a_n) \mid a_i \in R_i\}$ and perform componentwise addition and multiplication; that is, define $(a_1, a_2, ..., a_n) + (b_1, b_2, ..., b_n) = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$ and $(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n)$. This ring is called the direct sum of $R_1, R_2, ..., R_n$.

Properties of Rings

Theorem 11.1: Let a, b, and c belong to a ring R. Then 1. $a0 = 0a = 0$. (easy) 2. $a(-b) = (-a)b = -(ab)$. (easy) 3. $(-a)(-b) = ab$. (easy, simply from above) 4. $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$. (easy…)

Furthermore, if R has a unity element 1, then 5. $(-1)a = -a$. (from above) 6. $(-1)(-1) = 1$. (from above…)

Theorem 11.2: If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique. (proof as before)

Integral Domains

Zero-Divisors

A zero-divisor is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Integral Domain

An integral domain is a commutative ring with unity and no zero-divisors.

Examples:

- The ring Z_n of integers modulo n is not an integral domain when n is not prime.
- The ring of integers is an integral domain.
- $Z \oplus Z$ is not an integral domain.

Theorem 12.1

Let a, b, and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

Proof: From $ab = ac$, we have $a(b-c) = 0$. Since $a \neq 0$, we must have $b-c = 0$. ■

Many authors prefer to define integral domains by the cancellation property—that is, as commutative rings with unity in which the cancellation property holds. This definition is equivalent to ours.

Fields

A field is a commutative ring with unity in which every nonzero element is a unit.

To verify that every field is an integral domain, observe that if a and b belong to a field with $a \neq 0$ and $ab = 0$, we can multiply both sides of the last expression by a^{-1} to obtain $b = 0$.

Theorem 12.2

A finite integral domain is a field. (proof as in groups)

Corollary

Z_n is a field if and only if n is prime.

Characteristic of a Ring

The characteristic of a ring R is the least positive integer n such that $nx = 0$ (Remember that this is adding x, n times) for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\operatorname{char} R$.

- Thus, the ring of integers has characteristic 0, and Z_n has characternistic n.
- An infinite ring can have a nonzero characteristic. Indeed, the ring $Z_2[x]$ of all polynomials with coefficients in Z_2 has characteristic 2. (Addition and multiplication are done as for polynomials with ordinary integer coefficients except that the coefficients are reduced modulo 2.)

Theorem 12.3

Let R be a ring with unity 1. If 1 has infinite order under addition, then the characteristic of R is 0. If 1 has order n under addition, then the characteristic of R is n.

Proof: Suppose that 1 has additive order n (as other case is straight forward). Then $n \cdot 1 = 0$, and n is the least positive integer with this property. So, for any x in R, we have $n \cdot x = x + x + \cdots + x$ (n summands) $= 1x + 1x + \cdots + 1x$ (n summands) $= (1 + 1 + \cdots + 1)x$ (n summands)$ = (n 1)x = 0x = 0.$ Thus, R has characteristic n.

Corollary: Characteristic of a subfield is same as that of field as unity of subfield is same as that of unity of field.

Proof: If u is any element of F satisfying $u^2 = u$, then either $u = 0$ or $u = 1$.

If K is a subring of F having unity e, possibly different from $1 \in F$, then $e^2 = ee = e$ by definition of unity. So either $e = 0$ or $e = 1$, because $e \in F$. The

case $e = 0$ is disallowed if K is a subfield, because in a field it is required that the unity is nonzero.

Theorem 12.4

The characteristic of an integral domain is 0 or prime.

Proof: By Theorem 12.3, it suffices to show that if the additive order of 1 is finite, it must be prime. Suppose that 1 has order n and that $n = st$, where $1 \leq s, t \leq n$. Then, as we know, $0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1)$.

So, $s \cdot 1 = 0$ or $t \cdot 1 = 0$. Since n is the least positive integer with the property that $n \cdot 1 = 0$, we must have $s = n$ or $t = n$. Thus, n is prime. ■

Thus characteristic of a field is 0 or prime.

Ideals and Factor Rings

Ideal

A subring A of a ring R is called a (two-sided) ideal of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A.

- So, a subring A of a ring R is an ideal of R if A "absorbs" elements from R—that is, if $rA \subseteq A$ and $Ar \subseteq A$ for all $r \in R$.
- An ideal A of R is called a proper ideal of R if A is a proper subset of R.
- If A is an ideal of a ring R and 1 belongs to A, then $A = R$.

Theorem 13.1

A nonempty subset A of a ring R is an ideal of R if

1. $a - b \in A$ whenever $a, b \in A$.
2. ra and ar are in A whenever $a \in A$ and $r \in R$.

Examples:

- For any ring $R, \{0\}$ and R are ideals of R. The ideal $\{0\}$ is called the trivial ideal.
- For any positive integer n, the set $nZ = \{0, \pm n, \pm 2n, ...\}$ is an ideal of Z.
- Let R be a commutative ring with unity and let $a \in R$. The set $\langle a \rangle = \{ra \mid r \in R\}$ is an ideal of R called the principal ideal generated by a.
- Let $R[x]$ denote the set of all polynomials with real coefficients and let A denote the subset of all polynomials with constant term 0. Then A is an ideal of $R[x]$ and $A = \langle x \rangle$.
- Let R be a commutative ring with unity and let $a_1, a_2, ..., a_n$ belong to R. Then $I = \langle a_1, a_2, ..., a_n \rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R\}$ is an ideal of R called the ideal generated by $a_1, a_2, ..., a_n$.

- Let $Z[x]$ denote the ring of all polynomials with integer coefficients and let I be the subset of $Z[x]$ of all polynomials with even constant terms. Then I is an ideal of $Z[x]$ and $I = \langle x, 2\rangle$.

Theorem 13.2 (Existence of Factor Rings)

Let R be a ring and let A be a subring of R. The set of cosets $\{r+A \mid r \in R\}$ is a ring under the operations $(s+A)+(t+A) = s+t+A$ and $(s+A)(t+A) = st+A$ if and only if A is an ideal of R.

Proof: We know that the set of cosets forms a group under addition. Once we know that multiplication is indeed a binary operation on the cosets, it is trivial to check that the multiplication is associative and that multiplication is distributive over addition. Hence, the proof boils down to showing that multiplication is well-defined if and only if A is an ideal of R. To do this, let us suppose that A is an ideal and let $s + A = s' + A$ and $t + A = t' + A$. Then we must show that $st + A = s't' + A$. Well, by definition, $s = s' + a$ and $t = t' + b$, where a and b belong to A. Then and so $st = (s' + a)(t' + b) = s't' + at' + s'b + ab$ (thus $st \in s't' + A$, alternatively),

$st + A = s't' + at' + s'b + ab + A = s't' + A$, since A absorbs $at' + s'b + ab$. Thus, multiplication is well-defined when A is an ideal.

On the other hand, suppose that A is a subring of R that is not an ideal of R. Then there exist elements $a \in A$ and $r \in R$ such that $ar \notin A$ or $ra \notin A$. For convenience, say $ar \notin A$. Consider the elements $a + A = 0 + A$ and $r + A$. Clearly, $(a + A)(r + A) = ar + A$ but $(0 + A)(r + A) = 0r + A = A$. Since $ar + A \neq A$, the multiplication is not well-defined and the set of cosets is not a ring.

Examples:

- $2Z/6Z = \{0 + 6Z, 2 + 6Z, 4 + 6Z\}$. Here the operations are essentially modulo 6 arithmetic. For example, $(4 + 6Z) + (4 + 6Z) = 2 + 6Z$ and $(4 + 6Z)(4 + 6Z) = 4 + 6Z$.
- Let $R = \{\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \mid a_i \in Z\}$ and let I be the subset of R consisting of matrices with even entries. It is easy to show that I is indeed an ideal of R. Consider the factor ring R/I. The interesting question about this ring is: What is its size? We claim R/I has 16 elements; in fact, $R/I = \{\begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} + I \mid r_i \in \{0, 1\}\}$
- Consider the factor ring of the Gaussian integers $R = Z[i]/\langle 2 - i\rangle$. (*Note:* $(a + bi)(2 - i)$ doesn't cover the complete $Z[i]$ as a, b have to be integers) What does this ring look like? Of course, the elements of R have the form $a + bi + \langle 2 - i\rangle$, where a and b are integers, but the important question

is: What do the distinct cosets look like? The fact that $2-i+\langle 2-i\rangle = 0+\langle 2-i\rangle$ means that when dealing with coset representatives, we may treat $2-i$ as equivalent to 0, so that $2=i$. For example, the coset $3+4i+\langle 2-i\rangle = 3+8+\langle 2-i\rangle = 11+\langle 2-i\rangle$. (or $4i = 4i-8+8$) Similarly, all the elements of R can be written in the form $a+\langle 2-i\rangle$, where a is an integer. But we can further reduce the set of distinct coset representatives by observing that when dealing with coset representatives, $2=i$ implies (by squaring both sides) that $4=-1$ or $5=0$ (actually $(2+i)(2-i)=5$). Thus, the coset $3+4i+\langle 2-i\rangle = 11+\langle 2-i\rangle = 1+5+5+\langle 2-i\rangle = 1+\langle 2-i\rangle$. In this way, we can show that every element of R is equal to one of the following cosets: $0+\langle 2-i\rangle, 1+\langle 2-i\rangle, 2+\langle 2-i\rangle, 3+\langle 2-i\rangle, 4+\langle 2-i\rangle$. Is any further reduction possible? To demonstrate that there is not, we will show that these five cosets are distinct. It suffices to show that $1+\langle 2-i\rangle$ has additive order 5. Since $5(1+\langle 2-i\rangle) = 5+\langle 2-i\rangle = 0+\langle 2-i\rangle, 1+\langle 2-i\rangle$ has order 1 or 5. If the order is actually 1, then $1+\langle 2-i\rangle = 0+\langle 2-i\rangle$, so $1\in\langle 2-i\rangle$ (which can be verified to be impossible). It should be clear that the ring R is essentially the same as the field Z_5.

- Let $R[x]$ denote the ring of polynomials with real coefficients. Since, $\langle x^2+1\rangle = \{f(x)(x^2+1) \mid f(x)\in R[x]\}$. Then $R[x]/\langle x^2+1\rangle = \{g(x)+\langle x^2+1\rangle \mid g(x)\in R[x]\} = \{ax+b+\langle x^2+1\rangle \mid a,b\in R\}$. To see this last equality, note that if $g(x)$ is any member of $R[x]$, then we may write $g(x)$ in the form $q(x)(x^2+1)+r(x)$

How is multiplication done? Since $x^2+1+\langle x^2+1\rangle = 0+\langle x^2+1\rangle$, one should think of x^2+1 as 0 or, equivalently, as $x^2=-1$. So, for example, $(x+3+\langle x^2+1\rangle)(2x+5+\langle x^2+1\rangle) = 2x^2+11x+15+\langle x^2+1\rangle = 11x+13+\langle x^2+1\rangle$. In view of the fact that the elements of this ring have the form $ax+b+\langle x^2+1\rangle$, where $x^2+\langle x^2+1\rangle = -1+\langle x^2+1\rangle$, it is perhaps not surprising that this ring turns out to be algebraically the same ring as the ring of complex numbers.

Prime Ideals and Maximal Ideals

A prime ideal A of a commutative ring R is a proper ideal of R such that $a,b\in R$ and $ab\in A$ imply $a\in A$ or $b\in A$. A maximal ideal of a commutative ring R is a proper ideal A of R such that, whenever B is an ideal of R and $A\subseteq B\subseteq R$, then $B=A$ or $B=R$.

Examples:

- Let n be an integer greater than 1. Then, in the ring of integers, the ideal nZ is prime if and only if n is prime. ($\{0\}$ is also a prime ideal of Z.)
- The ideal $\langle x^2+1\rangle$ is maximal in $R[x]$. To see this, assume that A is an ideal of $R[x]$ that properly contains $\langle x^2+1\rangle$. We will prove that $A=R[x]$ by showing that A contains some nonzero real number c. Then $1=(1/c)c\in A$ and therefore, $A=R[x]$. To this end, let $f(x)\in A$, but

$f(x) \notin \langle x^2+1\rangle$. Then $f(x) = q(x)(x^2+1) + r(x)$, where $r(x) \neq 0$ and the degree of $r(x)$ is less than 2. It follows that $r(x) = ax + b$, where a and b are not both 0, and $ax + b = r(x) = f(x) - q(x)(x^2+1) \in A$. Thus, $a^2x^2 - b^2 = (ax+b)(ax-b) \in A$ and $a^2(x^2+1) \in A$. So, $0 \neq a^2 + b^2 = (a^2x^2 + a^2) - (a^2x^2 - b^2) \in A$.

- The ideal $\langle x^2+1\rangle$ is not prime in $Z_2[x]$, since it contains $(x+1)^2 = x^2 + 2x + 1 = x^2 + 1$ but does not contain $x + 1$.

Theorem 13.3

Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is an integral domain if and only if A is prime. (easy to prove)

Proof:

Suppose that R/A is an integral domain and $ab \in A$. Then $(a + A)(b + A) = ab+A = A$, the zero element of the ring R/A. So, either $a+A = A$ or $b+A = A$; that is, either $a \in A$ or $b \in A$. Hence, A is prime.

To prove the other half of the theorem, we first observe that R/A is a commutative ring with unity for any proper ideal A. Thus, our task is simply to show that when A is prime, R/A has no zero-divisors. So, suppose that A is prime and $(a + A)(b + A) = 0 + A = A$. Then $ab \in A$ and, therefore, $a \in A$ or $b \in A$. Thus, one of $a + A$ or $b + A$ is the zero coset in R/A.

Theorem 13.4

Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.

Proof:

Suppose that R/A is a field and B is an ideal of R that properly contains A. Let $b \in B$ but $b \notin A$. Then $b + A$ is a nonzero element of R/A and, therefore, there exists an element $c+A$ such that $(b+A)(c+A) = 1+A$, the multiplicative identity of R/A. Since $b \in B$, we have $bc \in B$. Because $1 + A = (b+A)(c+A) = bc+A$,

we have $1 - bc \in A \subset B$. So, $1 = (1 - bc) + bc \in B$. Thus, $B = R$. This proves that A is maximal.

Now suppose that A is maximal and let $b \in R$ but $b \notin A$. It suffices to show that $b+A$ has a multiplicative inverse. (All other properties for a field follow trivially.) Consider $B = \{br + a \mid r \in R, a \in A\}$. This is an ideal of R that properly contains A (easy to see). Since A is maximal, we must have $B = R$. Thus, $1 \in B$, say, $1 = bc+a'$, where $a' \in A$. Then $1+A = bc+a'+A = bc+A = (b+A)(c+A)$.

When a commutative ring has a unity, it follows from Theorems 13.3 and 13.4 that a maximal ideal is a prime ideal. The next example shows that a prime ideal need not be maximal.

Examples:

- The ideal $\langle x \rangle$ is a prime ideal in $Z[x]$ but not a maximal ideal in $Z[x]$. To verify this, we begin with the observation that $\langle x \rangle = \{f(x) \in Z[x] \mid f(0) = 0\}$. Thus, if $g(x)h(x) \in \langle x \rangle$, then $g(0)h(0) = 0$. And since $g(0)$ and $h(0)$ are integers, we have $g(0) = 0$ or $h(0) = 0$. To see that $\langle x \rangle$ is not maximal, we simply note that $\langle x \rangle \subset \langle x, 2 \rangle \subset Z[x]$

Ring Homomorphisms

A ring homomorphism ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all a, b in R,

$\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$.

A ring homomorphism that is both one-to-one and onto is called a ring isomorphism.

Examples:

- The correspondence $\phi : x \to 5x$ from Z_4 to Z_{10} is a ring homomorphism. Although showing that $\phi(x+y) = \phi(x)+\phi(y)$ appears to be accomplished by the simple statement that $5(x + y) = 5x + 5y$, we must bear in mind that the addition on the left is done modulo 4, whereas the addition on the right and the multiplication on both sides are done modulo 10. An analogous difficulty arises in showing that ϕ preserves multiplication. So, to verify that ϕ preserves both operations, we write $x + y = 4q_1 + r_1$ and $xy = 4q_2 + r_2$. Then $\phi(x + y) = \phi(r_1) = 5r_1 = 5(x + y - 4q_1)$ $= 5x + 5y - 20q_1 = 5x + 5y = \phi(x) + \phi(y)$ in Z_{10} . Similarly, using the fact that $5 \cdot 5 = 5$ in Z_{10} , we have $\phi(xy) = \phi(r_2) = 5r_2 = 5(xy - 4q_2)$ $= 5xy - 20q_2 = (5 \cdot 5)xy = 5x5y = \phi(x)\phi(y)$ in Z_{10}.
- We determine all ring homomorphisms from Z_{12} to Z_{30}. By Example in Chapter 10, the only group homomorphisms from Z_{12} to Z_{30} are $x \to ax$, where $a = 0$, 15, 10, 20, 5, or 25. But, since $1 \cdot 1 = 1$ in Z_{12}, we must have $a \cdot a = a$ in Z_{30}. This requirement rules out 20 and 5 as possibilities for a. Finally, simple calculations show that each of the remaining four choices does yield a ring homomorphism.
- An integer n with decimal representation $a_k a_{k-1} \cdots a_0$ is divisible by 9 if and only if $a_k + a_{k-1} + \cdots + a_0$ is divisible by 9. To verify this, observe that $n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_0$. Then, letting α denote the natural homomorphism from Z to Z_9 ($z \to z \bmod 9$) [in particular, $\alpha(10) = 1$], we note that n is divisible by 9 if and only if $0 = \alpha(n) = \alpha(a_k)(\alpha(10))^k +$ $\alpha(a_{k-1})(\alpha(10))^{k-1} + \cdots + \alpha(a_0) = \alpha(a_k) + \alpha(a_{k-1}) + \cdots + \alpha(a_0) = \alpha(a_k +$ $a_{k-1} + \cdots + a_0)$. But $\alpha(a_k + a_{k-1} + \cdots + a_0) = 0$ is equivalent to $a_k + a_{k-1} +$ $\cdots + a_0$ being divisible by 9.

- Let m be a fixed positive integer. For any integer a, let $\overline{a}$ denote a mod m. It is easy to see that the mapping $\phi : Z[x] \to Zm[x]$ given by $\phi(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) = \overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_0}$ is a ring homomorphism.

Theorem 14.1

Let ϕ be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S. (All below mentioned are super easy to prove)

1. For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.
2. $\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S.
3. If A is an ideal and ϕ is onto S, then $\phi(A)$ is an ideal.
4. $\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R.
5. If R is commutative, then $\phi(R)$ is commutative.
6. If R has a unity 1, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S.
7. ϕ is an isomorphism if and only if ϕ is onto and $\operatorname{Ker}\phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$.
8. If ϕ is an isomorphism from R onto S, then ϕ^{-1} is an isomorphism from S onto R.

Corollary: Let ϕ be a ring homomorphism from a ring R to a ring S. Then $\operatorname{Ker}\phi$ is an ideal of R.

Theorem 14.2 (First Isomorphism theorem for Rings)

Let ϕ be a ring homomorphism from R to S. Then the mapping from $R/\operatorname{Ker}\phi$ to $\phi(R)$, given by $r + \operatorname{Ker}\phi \to \phi(r)$, is an isomorphism. In symbols, $R/\operatorname{Ker}\phi \approx \phi(R)$.

Theorem 14.3

Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular, an ideal A is the kernel of the mapping $r \to r + A$ from R to R/A.

Examples:

- Since the mapping ϕ from $Z[x]$ onto Z given by $\phi(f(x)) = f(0)$ is a ring homomorphism with $\operatorname{Ker}\phi = \langle x \rangle$, we have, by Theorem 14.3, $Z[x]/\langle x \rangle \approx Z$. And because Z is an integral domain but not a field, we know by Theorems 13.3 and 13.4 that the ideal $\langle x \rangle$ is prime but not maximal in $Z[x]$.

Theorem 14.4

Let R be a ring with unity 1. The mapping $\phi : Z \to R$ given by $n \to n \cdot 1$ is a ring homomorphism.

Proof We have $\phi(m + n) = (m + n) \cdot 1 = m \cdot 1 + n \cdot 1$. So, ϕ preserves addition. That ϕ also preserves multiplication follows from Example done before, which says that $(m \cdot a)(n \cdot b) = (mn) \cdot (ab)$ for all integers m and n. Thus, $\phi(mn) = (mn) \cdot 1 = (mn) \cdot ((1)(1)) = (m \cdot 1)(n \cdot 1) = \phi(m)\phi(n)$. So, ϕ preserves multiplication as well.

Corollary 1: If R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to Z_n. If the characteristic of R is 0, then R contains a subring isomorphic to Z.

Proof: Let 1 be the unity of R and let $S = \{k \cdot 1 \mid k \in Z\}$. Theorem 14.4 shows that the mapping ϕ from Z to S given by $\phi(k) = k \cdot 1$ is a homomorphism, and by the First Isomorphism Theorem for rings, we have $Z/\operatorname{Ker}\phi \approx S$. But, clearly, $\operatorname{Ker}\phi = \langle n \rangle$, where n is the additive order of 1 and, by Theorem 12.3, n is also the characteristic of R. So, when R has characteristic n, $S \approx Z/\langle n \rangle \approx Z_n$. When R has characteristic 0, $S \approx Z/\langle 0 \rangle \approx Z$.

Corollary 2: For any positive integer m, the mapping of $\phi : Z \to Z_m$ given by $x \to x \bmod m$ is a ring homomorphism.

Proof: This follows directly from the statement of Theorem 14.4, since in the ring Z_m, the integer $x \bmod m$ is $x \cdot 1$.

Corollary 3: If F is a field of characteristic p, then F contains a subfield isomorphic to Z_p . If F is a field of characteristic 0, then F contains subfield isomorphic to the rational numbers.

Proof: By Corollary 1, F contains a subring isomorphic to Z_p if F has characteristic p, and F has a subring S isomorphic to Z if F has characteristic 0. In the latter case, let $T = \{ab^{-1} \mid a, b \in S, b \neq 0\}$. Then T is isomorphic to the rationals (Let ϕ be the isomorphism from S to Z, define $T(ab^{-1}) = \phi(a)/\phi(b)$). ■

Since the intersection of all subfields of a field is itself a subfield, every field has a smallest subfield (that is, a subfield that is contained in every subfield). This subfield is called the prime subfield of the field. It follows from Corollary 3 that the prime subfield of a field of characteristic p is isomorphic to Z_p, whereas the prime subfield of a field of characteristic 0 is isomorphic to Q.

Theorem 14.4

Let D be an integral domain. Then there exists a field F (called the field of quotients of D) that contains a subring isomorphic to D.

Proof: Let $S = \{(a, b) \mid a, b \in D, b \neq 0\}$. We define an equivalence relation on S by $(a, b) \equiv (c, d)$ if $ad = bc$. Now, let F be the set of equivalence classes of S under the relation $\equiv$ and denote the equivalence class that contains (x, y) by x/y. We define addition and multiplication on F by $a/b + c/d = (ad + bc)/(bd)$ and $a/b \cdot c/d = (ac)/(bd)$. (Notice that here we need the fact that D is an integral domain to ensure that multiplication is closed; that is, $bd \neq 0$ whenever $b \neq 0$ and $d \neq 0$.) Since there are many representations of any particular element of F (just as in the rationals, we have $1/2 = 3/6 = 4/8$), we must show that these two operations are well-defined. To do this, suppose that $a/b = a'/b'$ and $c/d = c'/d'$, so that $ab' = a'b$ and $cd' = c'd$. It then follows that $(ad+bc)b'd' = adb'd' + bcb'd' = (ab')dd' + (cd')bb' = (a'b)dd' + (c'd)bb' = a'd'bd + b'c'bd = (a'd' + b'c')bd$. Thus, by definition, we have $(ad+bc)/(bd) = (a'd' + b'c')/(b'd')$, and, therefore, addition is well-defined. Similarly, multiplication is well-defined. That F is a field is straightforward. Let 1 denote the unity of D. Then $0/1$ is the additive identity of F. The additive inverse of a/b is $-a/b$; the multiplicative inverse of a nonzero element a/b is b/a. The remaining field properties can be checked easily. Finally, the mapping $\phi : D \to F$ given by $x \to x/1$ is a ring isomorphism from D to $\phi(D)$

When F is a field, the field of quotients of $F[x]$ is traditionally denoted by $F(x)$.

Let p be a prime. Then $Z_p(x) = \{f(x)/g(x) \mid f(x), g(x) \in Z_p[x], g(x) \neq 0\}$ is an infinite field of characteristic p.

Polynomial Rings

Let R be a **commutative ring**. The set of formal symbols $R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0 \mid a_i \in R, n \text{ is a nonnegative integer } \}$ is called the ring of polynomials over R in the indeterminate x. Two elements $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0$ and $b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x^1 + b_0$ of $R[x]$ are considered equal if and only if $a_i = b_i$ for all nonnegative integers i. (Define $a_i = 0$ when $i > n$ and $b_i = 0$ when $i > m$.)

one must be careful not to confuse a polynomial with the function determined by a polynomial. For example, in $Z_3[x]$, the polynomials $f(x) = x$ and $g(x) = x^3$ determine the same function from Z_3 to Z_3, since $f(a) = g(a)$ for all a in Z_3. But $f(x)$ and $g(x)$ are different elements of $Z_3[x]$.

To make $R[x]$ into a ring, we define addition and multiplication in the usual way.

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x^1 + a_0$ and $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x^1 + b_0$ belong to $R[x]$. Then $f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \cdots + (a_1 + b_1)x + a_0 + b_0$, where s is the maximum of m and n. Also, $f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots 1c_1 x + c_0$, where $c_k = a_k b_0 + a_{k-1}b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$ for $k = 0, ..., m + n$.

Theorem 15.1

If D is an integral domain, then $D[x]$ is an integral domain.

Proof:

Since we already know that $D[x]$ is a ring, all we need to show is that $D[x]$ is commutative with a unity and has no zero-divisors. Clearly, $D[x]$ is commutative whenever D is. If 1 is the unity element of D, it is obvious that $f(x) = 1$ is the unity element of $D[x]$. Finally, suppose that $f(x) = a_n x_n + a_{n-1}x_{n-1} + \cdots + a_0$ and $g(x) = b_m x_m + b_{m-1}x_{m-1} + \cdots + b_0$, where $a_n \neq 0$ and $b_m \neq 0$. Then, by definition, $f(x)g(x)$ has leading coefficient $a_n b_m$ and, since D is an integral domain, $a_n b_m \neq 0$.

Theorem 15.2

Let F be a field and let $f(x), g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Proof: We begin by showing the existence of $q(x)$ and $r(x)$. If $f(x) = 0$ or $\deg f(x) < \deg g(x)$, we simply set $q(x) = 0$ and $r(x) = f(x)$. So, we may assume that $n = \deg f(x) \geq \deg g(x) = m$ and let $f(x) = a_n x_n + \cdots + a_0$ and $g(x) = b_m x_m + \cdots + b_0$. The idea behind this proof is to begin just as if you were going to "long divide" $g(x)$ into $f(x)$, then use the Second Principle of Mathematical Induction on $\deg f(x)$ to finish up. Thus, resorting to long division, we let $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x)$. Then, $f_1(x) = 0$ or $\deg f_1(x) < \deg f(x)$; so, by our induction hypothesis, there exist $q_1(x)$ and $r_1(x)$ in $F[x]$ such that $f_1(x) = g(x)q_1(x) + r_1(x)$, where $r_1(x) = 0$ or $\deg r_1(x) < \deg g(x)$. [Technically, we should get the induction started by proving the case in which $\deg f(x) = 0$, but this is trivial.] Thus, $f(x) = a_n b_m^{-1} x^{n-m} g(x) + f_1(x) = a_n b_m^{-1} x^{n-m} g(x) + q_1(x)g(x) + r_1(x) = [a_n b_m^{-1} x^{n-m} + q_1(x)]g(x) + r_1(x)$. So, the polynomials $q(x) = a_n b_m^{-1} x^{n-m} + q_1(x)$ and $r(x) = r_1(x)$ have the desired properties. Proving uniqueness is easy. ■

When the ring of coefficients of a polynomial ring is a field, we can use the long division process to determine the quotient and remainder.

Let D be an integral domain. If $f(x)$ and $g(x) \in D[x]$, we say that $g(x)$ divides $f(x)$ in $D[x]$ [and write $g(x)|f(x)$] if there exists an $h(x) \in D[x]$ such that $f(x) = g(x)h(x)$. In this case, we also call $g(x)$ a factor of $f(x)$. An element a is a zero (or a root) of a polynomial $f(x)$ if $f(a) = 0$.

When F is a field, $a \in F$, and $f(x) \in F[x]$, we say that a is a zero of multiplicity k ($k \geq 1$) if $(x-a)^k$ is a factor of $f(x)$ but $(x-a)^{k+1}$ is not a factor of $f(x)$.

Corollary 1: (Remainder Theorem) Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

Corollary 2: (Factor Theorem) Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

Corollary 3: A polynomial of degree n over a field has at most n zeros, counting multiplicity.

Proof: We proceed by induction on n. Clearly, a polynomial of degree 0 over a field has no zeros. Now suppose that $f(x)$ is a polynomial of degree n over a field and a is a zero of $f(x)$ of multiplicity k. Then, $f(x) = (x-a)^k q(x)$ and $q(a) \neq 0$; and, since $n = \deg f(x) = \deg(x-a)^k q(x) = k + \deg q(x)$, we have $k \leq n$ (As o/w…). If $f(x)$ has no zeros other than a, we are done. On the other hand, if $b \neq a$ and b is a zero of $f(x)$, then $0 = f(b) = (b-a)^k q(b)$, so that b is also a zero of $q(x)$ with the same multiplicity as it has for $f(x)$.

By the Second Principle of Mathematical Induction, we know that $q(x)$ has at most $\deg q(x) = n - k$ zeros, counting multiplicity. Thus, $f(x)$ has at most $k + n - k = n$ zeros, counting multiplicity.

A principal ideal domain is an integral domain R in which every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some a in R.

Theorem 15.3

Let F be a field. Then $F[x]$ is a principal ideal domain.

Proof: By Theorem 15.1, we know that $F[x]$ is an integral domain. Now, let I be an ideal in $F[x]$. If $I = \{0\}$, then $I = \langle 0 \rangle$. If $I \neq \{0\}$, then among all the elements of I, let $g(x)$ be one of minimum degree. We will show that $I = \langle g(x) \rangle$. Since $g(x) \in I$, we have $\langle g(x) \rangle \subseteq I$. Now let $f(x) \in I$. Then, by the division algorithm, we may write $f(x) = g(x)q(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Since $r(x) = f(x) - g(x)q(x) \in I$, the minimality of $\deg g(x)$ implies that the latter condition cannot hold. So, $r(x) = 0$ and, therefore, $f(x) \in \langle g(x) \rangle$. This shows that $I \subseteq \langle g(x) \rangle$.

Examples:

- Consider the homomorphism ϕ from $R[x]$ onto C given by $\phi(x) \to \phi(i)$ (that is, evaluate a polynomial in $R[x]$ at i). Then $x^2 + 1 \in \operatorname{Ker} \phi$ and is clearly a polynomial of minimum degree in $\operatorname{Ker} \phi$. Thus, $\operatorname{Ker} \phi = \langle x^2 + 1 \rangle$ and $R[x]/\langle x^2 + 1 \rangle$ is isomorphic to C.

Factorization of Polynomials

Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be irreducible over D if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called reducible over D.

Note that polynomial of degree ≥ 1 is never a unit due to the way multiplication is defined.

In the case that an integral domain is a field F, it is equivalent and more convenient to define a nonconstant $f(x) \in F[x]$ to be irreducible if $f(x)$ cannot be expressed as a product of two polynomials of lower degree.

Examples:

- The polynomial $f(x) = 2x^2 + 4$ is irreducible over Q but reducible over Z, since $2x^2 + 4 = 2(x^2 + 2)$ and neither 2 nor $x^2 + 2$ is a unit in $Z[x]$.
- The polynomial $f(x) = 2x^2 + 4$ is irreducible over R but reducible over C.
- The polynomial $x^2 - 2$ is irreducible over Q but reducible over R.
- The polynomial $x^2 + 1$ is irreducible over Z_3 but reducible over Z_5 as $(x^2 + 1) = (x + 3)(x + 2)$. Also note that zero of $x^2 + 1$ in Z_5 is 2.

In general, it is a difficult problem to decide whether or not a particular polynomial is reducible over an integral domain, but there are special cases when it is easy.

Theorem 16.1: Let F be a field. If $f(x) \in F[x]$ and $\deg f(x)$ is 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

Proof: Suppose that $f(x) = g(x)h(x)$, where both $g(x)$ and $h(x)$ belong to $F[x]$ and have degrees less than that of $f(x)$. Since $\deg f(x) = \deg g(x) + \deg h(x)$ and $\deg f(x)$ is 2 or 3, at least one of $g(x)$ and $h(x)$ has degree 1. Say $g(x) = ax + b$. Then, clearly, $-a^{-1}b$ is a zero of $g(x)$ and therefore a zero of $f(x)$ as well. Conversely, suppose that $f(a) = 0$, where $a \in F$. Then, by the Factor Theorem, we know that $x - a$ is a factor of $f(x)$ and, therefore, $f(x)$ is reducible over F. ■

So, in case of Z_p, we can easily check for reducibility of $f(x)$ by testing if $f(a) = 0$ for $a = 0, 1, ..., p - 1$.

The content of a nonzero polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where the $a's$ are integers, is the greatest common divisor of the integers $a_n, a_{n-1}, ..., a_0$. A primitive polynomial is an element of $Z[x]$ with content 1.

Gauss's Lemma: The product of two primitive polynomials is primitive.

Proof: Let $f(x)$ and $g(x)$ be primitive polynomials, and suppose that $f(x)g(x)$ is not primitive. Let p be a prime divisor of the content of $f(x)g(x)$, and let $\overline{f(x)}, \overline{g(x)}$, and $\overline{f(x)g(x)}$ be the polynomials obtained from $f(x)$, $g(x)$, and $f(x)g(x)$ by reducing the coefficients modulo p. Then, $\overline{f(x)}$ and $\overline{g(x)}$ belong to the integral domain $Z_p[x]$ and $\overline{f(x)}\,\overline{g(x)} = \overline{f(x)g(x)} = 0$, the zero element of $Z_p[x]$. Thus, $\overline{f(x)} = 0$ or $\overline{g(x)} = 0$. This means that either p divides every coefficient of $f(x)$ or p divides every coefficient of $g(x)$. Hence, either $f(x)$ is not primitive or $g(x)$ is not primitive. This contradiction completes the proof. ■

Theorem 16.2: Let $f(x) \in Z[x]$. If $f(x)$ is reducible over Q, then it is reducible over Z.

Proof: Suppose that $f(x) = g(x)h(x)$, where $g(x)$ and $h(x) \in Q[x]$. Clearly, we may assume that $f(x)$ is primitive because we can divide both $f(x)$ and $g(x)$ by the content of $f(x)$. Let a be the least common multiple of the denominators of the coefficients of $g(x)$, and b the least common multiple of the denominators of the coefficients of $h(x)$. Then $abf(x) = ag(x) \cdot bh(x)$, where $ag(x)$ and $bh(x) \in Z[x]$. Let c_1 be the content of $ag(x)$ and let c_2 be the content of $bh(x)$. Then $ag(x) = c_1 g_1(x)$ and $bh(x) = c_2 h_1(x)$, where both $g_1(x)$ and $h_1(x)$ are primitive, and $abf(x) = c_1 c_2 g_1(x)h_1(x)$. Since $f(x)$ is primitive, the content of $abf(x)$ is ab. Also, since the product of two primitive polynomials is primitive, it follows that the content of $c_1c_2g_1(x)h_1(x)$ is c_1c_2. Thus, $ab = c_1c_2$ and $f(x) = g_1(x)h_1(x)$, where $g_1(x)$ and $h_1(x) \in Z[x]$ and $\deg g_1(x) = \deg g(x)$ and $\deg h_1(x) = \deg h(x)$. ■

Example:

- For the polynomial $f(x) = 6x^2 + x - 2 = (3x - 3/2)(2x + 4/3) = g(x)h(x)$. In this case we have $a = 2, b = 3, c_1 = 3, c_2 = 2, g_1(x) = 2x - 1$, and $h_1(x) = 3x + 2$.

Irreducibility Tests

Theorem 16.3: Let p be a prime and suppose that $f(x) \in Z[x]$ with $\deg f(x) \geq 1$. Let $\bar{f}(x)$ be the polynomial in $Z_p[x]$ obtained from $f(x)$ by reducing pall the coefficients of $f(x)$ modulo p. If $\bar{f}(x)$ is irreducible over Z_p and $\deg \bar{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over Q.

Proof: It follows from the proof of Theorem 16.2 that if $f(x)$ is reducible over Q, then $f(x) = g(x)h(x)$ with $g(x), h(x) \in Z[x]$, and both $g(x)$ and $h(x)$ have degree less than that of $f(x)$. Let $\bar{f}(x), \bar{g}(x)$, and $\bar{h}(x)$ be the polynomials obtained from $f(x), g(x)$, and $h(x)$ by reducing all the coefficients modulo p. Since $\deg f(x) = \deg \bar{f}(x)$, we have $\deg \bar{g}(x) \leq \deg g(x) < \deg \bar{f}(x)$ and $\deg \bar{h}(x) \leq \deg h(x) < \deg \bar{f}(x)$. But, $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$, and this contradicts our assumption that $\bar{f}(x)$ is irreducible over Z_p. ■

Advanced Group Theory Results

Chinese Remainder Theorem

Given $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \in \mathbb{Z}$ and $gcd(a_i, a_j) = 1 \forall i \neq j$. Find a s.t. $a = b_i \bmod a_i$

Solution:

Define $p_i = \prod_{j \neq i} a_j$

then $p_i \begin{cases} \equiv 0 (\mathrm{mod} a_j) \text{ if } j \neq i \\ \not\equiv 0 (\mathrm{mod} a_i) \end{cases}$

We have,

$(\prod_{j \neq i} a_j) \bmod a_i \in U(a_i)$ (as they are relatively prime) $\rightarrow \exists c_i$ s.t. $c_i(\prod_{j \neq i} a_j) \equiv 1 \bmod a_i$

$\rightarrow a = \sum b_i (c_i \prod_{j \neq i} a_j)$

Mentioning without proof that such a solution is unique modulo $\prod a_j$

Theorem AG.1:

$U(m)$ is cyclic precisely if $m \in \{2, 4, p^r, 2p^r\}$, where $p \neq 2$ and is prime.

Proof:

Case 1: $m = 2^r; r > 2$

Let $\lambda = 2^{r-1} - 1, \beta = 2^r - 1$

$\lambda^2 = 2^{2r-2} + 1 - 2^r = 1$

And

$\beta^2 = 2^{2r} + 1 - 2^{r+1} = 1$

Thus $U(m)$ is not cyclic.

Case 2: $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, r > 1$

Define $\lambda_i \begin{cases} \equiv p_i^{a_i} - 1 \bmod p_i^{a_i} \\ \equiv 1 \bmod p_j^{a_j} \text{ and } (j \neq i) \end{cases}$

Note that if $p_i = 2$ and $a_1 = 1$ then both equivalence will become same and hence following arguments will not be valid.

Which we can easily find using CRT.

Now, $\lambda_i^2 \equiv 1 \bmod p_j^{a_j} \rightarrow \lambda_i^2 \equiv 1 \bmod m \forall i \rightarrow \lambda_i^2 - 1$ is divisible by m.

$\{\overline{\lambda_1}, \dots, \overline{\lambda_r}\} \subset U(m)$ where $\overline{\lambda_i} = \lambda_i \bmod m$ and is such that $\overline{\lambda_i} \neq \overline{\lambda_j}$ and $\overline{\lambda_i}^2 \equiv \overline{\lambda_j}^2 \equiv 1 \bmod m$

Therefore $U(m)$ is not cyclic.

Group Action

If G is a group and S is a set of objects, we say that G acts on S if there is a homomorphism ψ from G to $sym(S)$ (or also denoted as $A(S)$), the group of all permutations on S.

Examples:

- Let S be a finite set of n elements, choose an enumeration of $S = \{s_1, s_2, \dots, s_n\}$ then we get an action of S_n on S, $\psi : S_n \rightarrow A(S), \psi(\sigma)(s_i) = s_{\sigma(i)}$.

Problems

- Let H be a subgroup of G. Define $L : G \rightarrow A(G/H), L(g)(aH) = gaH$. Clearly this is an homomorphism. What is $\text{Ker}(L)$?

  Sol: $gaH = aH \rightarrow ga \in aH \rightarrow g \in aHa^{-1}$. So answer is intersection fo all conjugates, i.e. $\text{Ker}(L) = \cap_{a \in G} aHa^{-1}$.

- G is a finite group, $H \subset G$ is a subgroup. Assume $|G| \nmid |i_G(H)|!$. Show that $\exists$ a normal subgroup $N \lhd H$ and $N \neq \{e\}$.

  Sol: Consider the homomorphism of above example, $L : G \rightarrow A(G/H) \approx S_{\frac{|G|}{|H|}}$, now since $n \nmid |A(G/H)|$ therefore L cannot be injective and hence $\text{Ker}(L) \neq \{e\}$, which is our required normal subgroup.

- Prove that a group of order p^2 (where p is prime) has a normal subgroup of order p.

  Sol: Let $H \subset G$ be any subgroup of order p. Since $p^2 \nmid |p|!$, $\therefore \text{Ker}(L) \neq \{e\}$ and since $\text{Ker}(L) \subseteq H$ but as $|H| = p \rightarrow \text{Ker}(L) = H$, $\therefore H$ is normal in G.

- If G is a non abelian group of order 6 then show that $G \approx S_3$.

  We know that it has an element of order 3 and 2. Let $H = \langle a \rangle$ be of order 3 (Thus as it's index is 2, it is normal subgroup). Let $K = \langle b \rangle$ be of order 2. Consider $L : G \to A(G/K)$, Now as $\text{Ker}(L) \trianglelefteq K$ and either $\text{Ker}(L) = e$ or $\text{Ker}(L) = K$.

  If $\text{Ker}\, L = K \to K \lhd G$ and $HK = G = \langle ab \rangle$, thus G is cyclic $\Rightarrow\Leftarrow$.

  And therefore $\text{Ker}\, L = \{e\}$, and therefore L is an isomorphism.